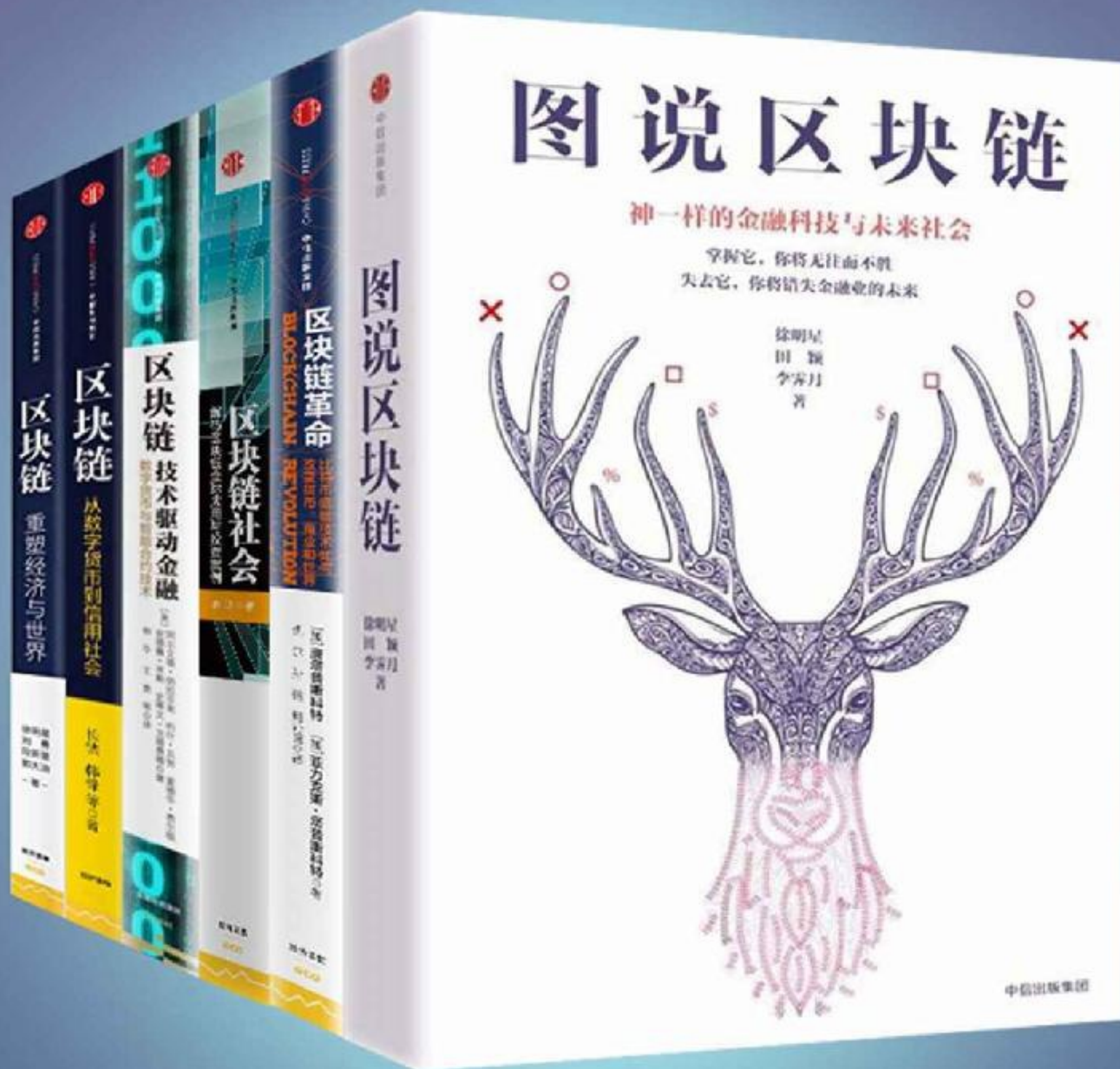


解码区块链

(套装共6册)



中信出版集团

www.aibbt.com 让未来触手可及

解码区块链全集（套装共6册）

徐明星 田颖 李霁月 [加]唐塔普斯科特 等 著
凯尔 孙铭 周沁园 等 译

中信出版社

目录

图说区块链

区块链革命：比特币底层技术如何改变货币、商业和世界

区块链社会：解码区块链全球应用与投资案例

区块链：技术驱动金融

区块链：从数字货币到信用社会

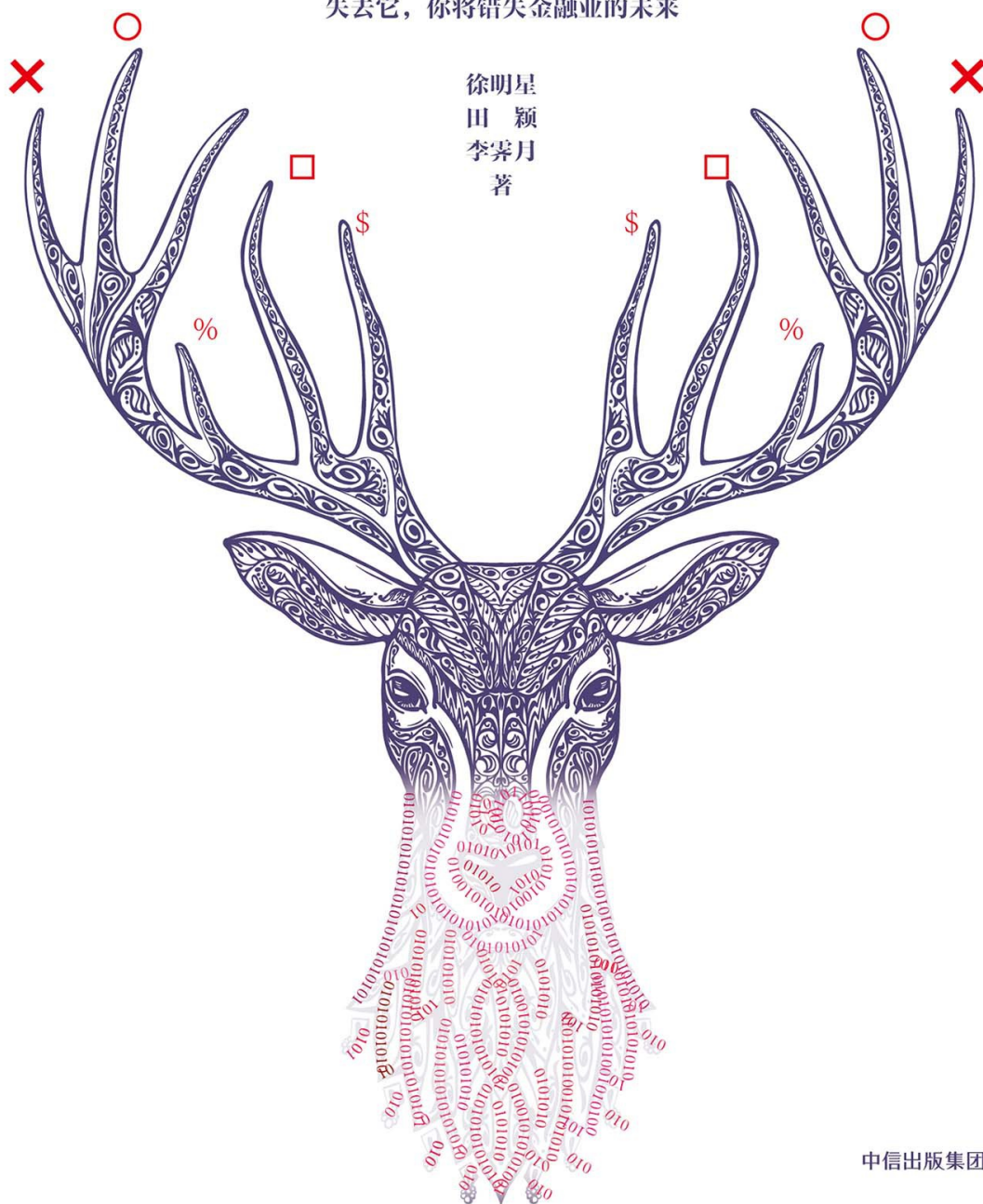
区块链：重塑经济与世界

图说区块链

神一样的金融科技与未来社会

掌握它，你将无往而不胜
失去它，你将错失金融业的未来

徐明星
田 颖
李霁月
著



中信出版集团

图说区块链

徐明星 田颖 李霖月 著

中信出版社

目录

推荐序一

推荐序二

01 起源篇

账本演变：一本账的兴衰发展史

价值转移：互联网之后还有什么

信用成本：你能记住多少人的脸

技术创新：从比特币到区块链

02 原理篇

讲一个故事，什么是区块链

讲一下原理，区块链如何运作

讲几个问题，区块链底层架构

03 人物篇

永远的背影：中本聪的99种传说

当尼克·萨博被自动售货机“砸中”

从华尔街走出的区块链女性领袖人物

在《纽约时报》撰写专栏的男子

想投资所有数字资产项目的大亨

04 应用篇

区块链+金融

区块链+互联网管理

区块链+能源

区块链+政府

区块链+医疗

区块链+版权

区块链+物联网

区块链+农业

区块链+慈善

区块链+其他

05 装备篇

比特币简史：从何处来往何处去

区块链词条：人手必备拿好不送

附录

在区块链创业公司做COO是一种什么体验？

区块链公司的“技术大牛”们是不是都怀着改变世界的梦想？

想要让你看懂抽象化的区块链我可能还差100个毕加索！

为了推广没人知道的区块链我们做了哪些疯狂的事？

致谢

推荐序一

夯实通往区块链社会的基础



这个时代变化太快！互联网金融刚刚热了几年，金融科技（FinTech）便取而代之。比特币的矿工和炒家们刚刚结伙成帮，区块链（Blockchain）便登堂入室形成“链圈”。一波波新概念让我们眼花缭乱，在不断鼓噪的创新颠覆中，莫名的焦虑感笼罩着所有人。极客们彼此创造深奥晦涩的词汇来建立行业壁垒，把自己弄得云里雾里，失去了与正常人沟通的能力。普通大众则马不停蹄地参加各种论坛沙龙，如饥似渴地汲取新知，唯恐坠入智能时代的底层。

我就是这样一个焦虑症患者，一直关注比特币挖矿、极客的算法逻辑和区块链先知们的布道，不时沉浸在瞬间的快乐和间歇性沮丧之中。面对所有变化——金融的、艺术的、科技的、社会的，我们都会坚定地向往和跟随这些创新，即便大多数会走向失败，过程却是充满着大大小小的快活之处。区块链也会是这样的。

2016年夏天我参加了加勒比海内克岛（Necker Island）的区块链三天恳谈会。著名嬉皮士企业家理查德·布兰森（Richard Branson）邀请了十几个国家不同领域的人士在海浪和阳光沙滩的环抱中讨论区块链的应用。没错，这种时空穿越真是让人惊喜。这些来自政府、法院、情报系统、互联网、艺术、航天和环保机构的30多位彼此陌生的人士组织了十几场不同主题的讨论会，讨论抓捕逃犯、防范洗钱、保护艺术产权、确

认交易真实性、防止贪污腐败、社会选举、地震救援和濒危生物的保护等，在感受到这些领域鲜活的具体成就的同时，也在体会一个共同的应用逻辑：这都是建立在大数据分析基础上自发组织、彼此交叉合作的成果，而且没有一个权威机构或企业在组织这个系统和过程。

按在场的一个年轻人的话，我们正在创造一个全新的信任协议，所有参与者都在编写制约我们行为的程序。没有上帝，没有国王，也没有政府和大公司这样的权威居高临下或者中心操控，而世界仍然在运行，而且更重要的是，革命正在发生。这个年轻人是亚历克斯·塔普斯科特，他刚刚与写过《维基经济学》等许多畅销书的父亲唐·塔普斯科特合作出版了新书《区块链革命》，现在其中文版在中国很畅销。2017年1月，我与唐·塔普斯科特同台担任嘉宾，并邀约其今年夏天来中国金融博物馆讲演。

当时在内克岛的人几乎没有一位是技术专家，没有一位是比特币挖矿者，没有人懂得哈希算法和双花理论，但大家都信心满满地讨论区块链。很简单，制作电视节目的人不必关心电视信号如何发射和显现，设计手机的人也不需要了解4G（第4代移动通信技术）的原理和每个零件的功能。对于打电话和看电视的消费者来说，更不必有什么深厚的技术储备。最后一天的晚会上，主持人提议所有人为区块链下一个定义，而且彼此不能重复，这真是有趣的游戏，几位来自非洲和德国的朋友，居然用歌声和Rap（说唱）来表达。几个核心词就是“信任”、“认证”和“价值转移”。区块链能实现价值转移，是超越信息转移的第二代互联网。当然，这只是当时的认知，今天我们已经大大丰富了对区块链的理解，而且每个人都拥有理解的权利，不需要来自某个权威的定义。

截至2017年3月，我可以在网上查到的区块链方面的中文书籍达到40种，估计还会有100本在2017年年底问世。如同当年互联网刚刚进入中国一样，普及书的泛滥也是浪潮的重要先声。当年的因特网和万维网等译名，陆续被互联网替代，极客们使用的区块链也可能被更好的译名

所替代。互联网金融博物馆在2016年曾发动了两轮译名讨论，我和许多同道中人更欣赏“公信链”，不过，我也同意许多从事金融监管的朋友的意见，在中国目前的环境下，“公信”一词有可能被非法集资者滥用，还是留给监管机构判定吧。

区块链脱胎于比特币，作为底层技术被发掘和推广。比特币引发了广泛的社会关注，特别在中国当下这样一个执着于赚钱赢利的功利环境下，比特币迅速在金融和投资领域深度演绎着系列故事，也立即被高度监管。不过，区块链技术则破土而出，独立形成了一个更广泛的应用空间。如同互联网的TCP/IP协议一样，如果你不执迷于解码和编码，你就可以发现区块链技术远比浏览互联网和电商交易有更为广泛和深刻的应用。许多人将区块链视为一个巨大的分布式记账体系，所有人参与记账查账，无人有能力篡改。这很有道理，但区块链显然要远远超过记账的认证功能。

区块链说到底更是一种观念，用技术设计取代权威控制和情感信任，以此建立一种网络结构，所有人都是可以参与成为无数节点之一，进行认证、确权、交易、追溯和调整等一系列动作，它公开透明，成本低、速度快、分布广，没有权威可以篡改伪造和取缔记录。我们可以充分想象今天的商业、艺术、司法、科技、政治乃至社会等各个领域，这样一个建立在运算能力和技术架构上的网络文明社会基础设施将是多么不同。尽管它毫无情怀和冰冷地运作，但从根本上摒弃了狂热理想的驱使、自命权威的霸道、垄断财团的曲扭、民粹阴谋的盲动，商业诈骗和情感敲诈也会随之水落石出。无论我们是否喜欢，区块链理念所驱动的全新社会正在迅速形成，不仅仅在比特币和金融科技领域。这是社会生态的巨大变化，也是许多人提到的革命意义。

比特币的开发者中本聪是一个时代的里程碑，但随着社会大数据的深厚积累，以及计算机能力的空前突破，社会网络的多元和复杂——特别是“80后”一代人的生活态度和自由选择精神，形成了区块链社会的核

心基础。我们也许很难预测区块链社会的未来支撑点，但它对我们现存社会生活方式的颠覆则是确定无疑的。重要的不再是对区块链的定义，而是我们如何了解和进入区块链社会。

区块链极客们开阔了我们的视野和思考逻辑，但区块链的广泛应用才是让无数学习者和创新者夯实通往区块链社会的条条大路。北京金融局率先支持区块链技术在防范非法集资和恶意诈骗领域的应用，推动中国区块链应用研究中心成为民间公益平台（2015年11月在北京成立，继而又开拓到浙江和上海等地）。2017年1月，中国区块链应用研究中心又组成代表团参加达沃斯论坛并参与创建了由25个成员组成的全球区块链商业理事会（GBBC），中国担任执行理事并主导区块链培训认证委员会，这是参与业界标准制定的重要机遇。

根据约定，中国区块链应用研究中心在2017年开始编制教材，开办面向区块链应用的公益性普及培训班，得到各界的广泛响应。仅经过三天的微信发布，就收到来自全国各地的170位朋友报名。中国保监会前副主席魏迎宁，中国区块链应用研究中心首任主席徐明星和新任主席邓迪等亲自授课，首期学员将得到全球区块链商业理事会和互联网金融博物馆的联合培训认证。目前，上海、珠海等地已经开始启动新一期培训。

区块链观念的普及和区块链应用的尝试取决于新一代创业者的积极参与，也取决于监管者的宽容和呵护。应本书编者邀请，我匆匆在其出版前写下寄语，期待与参与培训的学员们一起珍惜贴近前沿的机缘，共同努力，为之添砖加瓦，夯实区块链社会的基础。

中国金融博物馆理事长 王巍

推荐序二

这是一本区块链普及读物



我们认识并改造这个世界的方式一直在改变，而技术是其中最大的推动力。

区块链从诞生时背后推手的神秘，到最近比特币达到天价的惊世骇俗，如今又改头换面成为金融变革的顶层设计，短短数年间，对它最高的评价已经是：可以和互联网的重要性并驾齐驱。

所有技术的普及所面临的最大难点是教育。在中国传播区块链的最早的一些圈子里，为了区块链这三个字的翻译及中文命名曾产生过一些小小的争议。为什么？因为区块链要达到互联网那样的家喻户晓，能够顾名思义极其重要。毕竟，区块链从字面上很难直观理解。而区块链技术的拥趸们又是多么渴望让这个技术像互联网一样进入寻常百姓家！于是，有关区块链的书籍如雨后春笋，比起那些技术内容特别高级的专著，这本书起到了为人指路的作用。

此书轻松浅显，图文并茂，让技术变得可爱与可亲，作者的良苦用心跃然纸上。读者从中既能感受到艰深技术名词背后的人文脉络，在不知不觉中掌握一个时髦的技术概念，又能获得在朋友圈指点区块链的知识储备，惠而不费。

当然，技术普及的道路并不轻而易举，即使在经过种种努力以后，

一些基本的技术理念还是需要读者去细细体会。建议读者尝试去金融博物馆看看比特币挖矿的机器，了解一下哈希密码为何难以破解，以及关注一些最新的区块链动态以跟上时代的脉搏。也许，你一辈子也不需要真正掌握这些高深莫测的技术，但当身边一切的信息和金融服务都发生在区块链上之时，你今天的一点点阅读时间，将帮助你更好地拥抱一个新的世界，理解一个新的记录历史、登记权利、转移价值的方式。

徐明星在比特币行业堪称华山论剑级别的剑客，早年的技术积累与极客般的敏锐使得其创办的比特币交易平台OKCoin在中国备受推崇。如今，为了更广泛地推广区块链技术，他撰写了此书，这将为区块链的普及带来一股清风。

点融网创始人、联合CEO 郭宇航

01 起源篇

试着下个定义，谈谈偶然背后的必然

金融科技，一个现象级概念，随着新兴互联网与科技产业的高速发展，金融科技创新迎来“奇点式”的发展。其中，最引人注目的无疑是区块链技术。区块链是未来5年最有前景的行业之一，是全球各大金融机构和顶级银行都在大力投资和追逐的新兴领域。

说到区块链，我们首先要讨论的问题就是“为什么”，为什么区块链会这么火？凭什么认为区块链可以改变世界？在写这一章节前，我拜读了许多老师的著作，例如《区块链革命》《区块链金融》《商业区块链》《区块链社会》《区块链重塑经济与世界》等。各位行业专家从经济、商业发展、人类历史、技术变革等多方面阐述了区块链兴起的原因和其背后的逻辑。细细读过之后，真的是深陷于区块链的魅力之中不能自拔，而在这一章中，我将会选出最让我震惊的区块链神奇逻辑的4个角度（账本演变、价值转移、信用成本、技术创新）来谈一谈，究竟区块链为何诞生又是为何而来？

账本演变：一本账的兴衰发展史

区块链是21世纪最前沿的现象级概念，概述区块链最直接的词汇就是“分布式账本”，那么，我们就先从记账演变的角度来探寻一下，区块链为什么会诞生，分布式账本技术又为什么会引起经济社会的变革？



图1-1 旧石器时代的记账

我们首先把时间回溯到遥远的旧石器时代，在数万年以前，人们记账全凭智商，今天猎取了几头羊，吃了几头牛，全部靠死记硬背和心算。

之后呢，随着部落的人数越来越多，生产力也越来越高，于是开始出现用不了的东西，也就是生产者剩余。这个时候，部落里的经济需求也复杂起来，单靠脑袋计数已经满足不了，于是，记录就成了必须要改善的事，人们发明了简单刻画和直观绘图两种方法。刻画就是用各种符号来记录，绘图就是把场景画下来。因此，记账的萌芽产生了。



图1-2 记账的萌芽：刻画和绘图

到了后来，部落的人越来越多，需要记账的东西也越来越多，绘画和刻画这些费力又占地方的记录方式完全跟不上需求。于是，家喻户晓的结绳记事出现了，说起结绳记事，不止史书，中学的历史教科书上也有提及。结绳记事对记录对象、数量变化、最终结果都形成了确定的表现形式。这个时候，我们可以看出，它已经表现出账簿记录的几个基本原理，这几乎可以称作账本的起源。

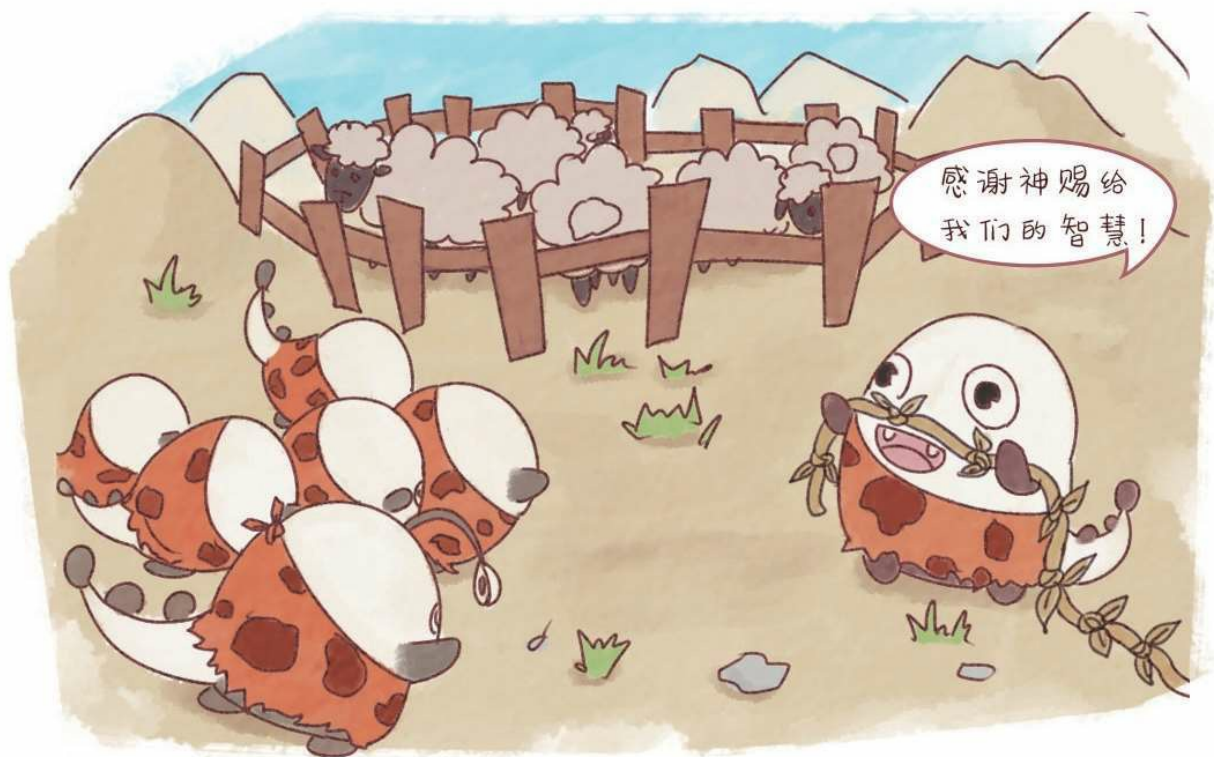


图1-3 记账的起源：结绳记事

到了原始社会末期，生产力发展到了前所未有的水平，剩余物品越来越多，农业、畜牧业、手工业分工扩大，文字出现了，人们开始使用书契等文字叙述式的会计记录法，收支事项按照时间的发生顺序形成了流水账。



图1-4 原始社会末期：流水账

之后，时间到了公元前5世纪，由于古希腊及古罗马奴隶社会的经济繁荣发展，流水账中出现了日记账和现金出纳账，也就是指按时间、物品名、人名、货币资金等分别设置的类似于账户的账本。这个时候，记账的历史就已经发展到了单式记账法时期。



图1-5 单式记账法时期

接下来，我们就来说一说流通相对比较广泛的复式记账法了。中国的复式记账法起源于明末清初的龙门账，之后又发展成四脚账；而西方的复式记账法最早出现在12—13世纪，它存在于意大利的一些商人和银行家之间。[\[1\]](#)复式记账法不仅能够核算经营成本，还可以分化出利润和资本，可以说它保证了企业经营的持续性。



图1-6 复式记账法时期

后来，到了19世纪，信息技术爆炸式发展，企业的所有者和经营者不再是一个人，大家都有看账本的需求，而且需要处理的工作也越来越复杂。比如我是这个企业最大的股东但是我不想管事，于是我聘请你作为职业经理人帮我管理这个公司，到了年终分红的时候，运营报告显示我该分得1 000万元，这个时候，我会说：“我想要看看账本。”

然后我一看，广告费投了3 000万元，比我一年挣的都多，于是我就开始怀疑你，这笔账你记得对不对啊，不会是乱写吧。不放心的我想出了一个办法，我雇用了一个由第三方协会认证的会计，专门负责帮我记账。这也就是记账历史的后续发展，当记账的需求增加，且存在着企业所有者与企业经营者因账目而引发的信任问题，会计这个职位就诞生了，之后，计算机技术的快速普及使会计行业走向了一个新的纪元，即会计电算化。



图1-7 19世纪：会计的诞生

到了21世纪这个信息化、数据化、智能化的世界，我们的记账手段不断完善和创新，但是仍然存在信息不对称及信用问题。举个最简单的例子，在没有得到完全正确的公开信息时，你要如何信任一个会计或审计给你的账目呢？你是否会怀疑事务所和公司勾结做假账？为了解决这样的问题，区块链给了我们一个新的选择，也就是比特币的底层应用，它可以被看作一个分布式共享的账本。

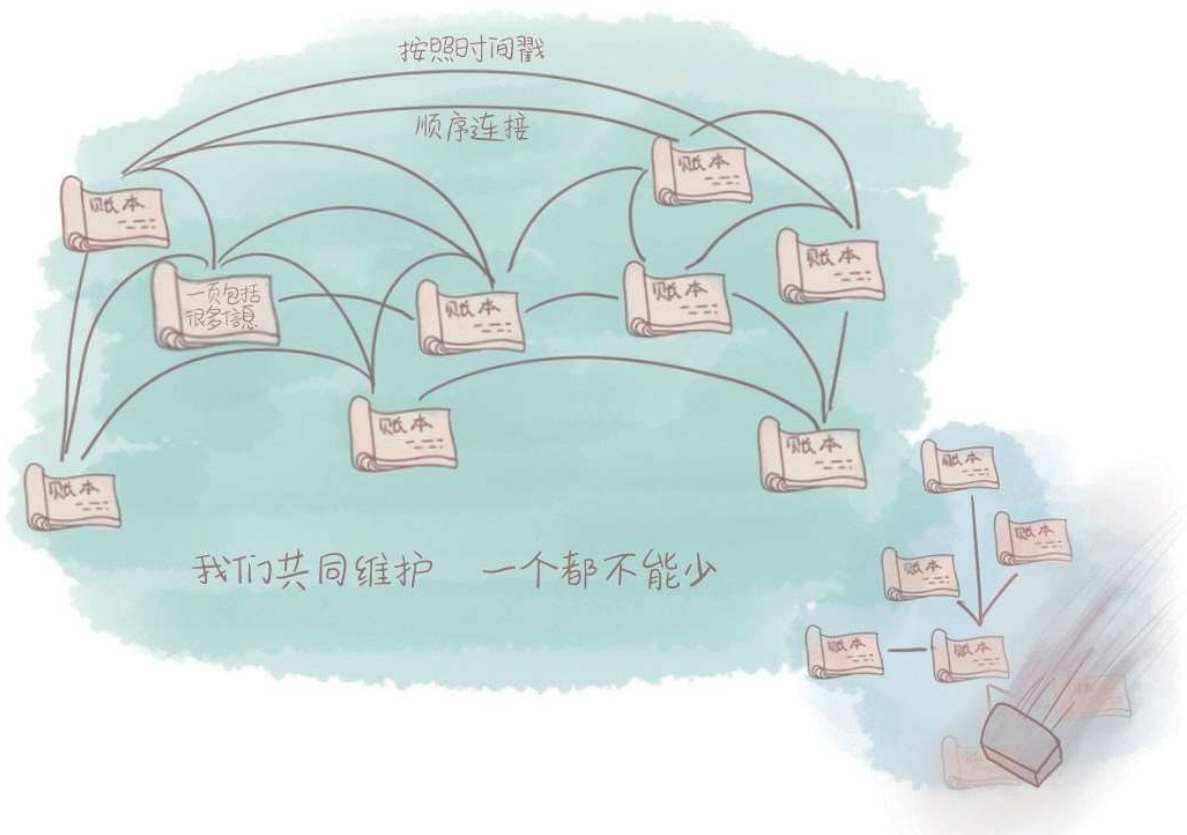


图1-8 分布式账本

从账本演变的角度来看，区块链是一个分布式共享的账本系统。这个账本有以下三个特点：

1. 可以无限增加的巨型账本——每个区块可以视作这个账本的一页，每增加一个区块，账本就多了一页，这一页中可能会包含一条或多条记录信息；
2. 加密且有顺序的账本——账目信息会被打包成一个区块并加密，同时盖上时间戳，一个个区块按时间戳顺序链接形成一个总账本；
3. 去中心化的账本——由网内用户共同维护的，它是去中心化的。

区块链是人类的记账历史走到现在，科技给我们的最新的选择，它是账本演变史上最新的一个高可行性的形态。

价值转移：互联网之后还有什么

互联网是我们已经不再陌生的概念，它渗入我们生活的方方面面，可以让信息高速、低成本地传输，是一条信息高速公路，但是，它却无法传递一类特殊的信息，那就是货币，而区块链恰恰可以解决这样的问题，因为区块链是一种价值传输网络。

我们先来看一下互联网的诞生，1993年，美国宣布了一项新的计划——国家信息基础设施，目的是建设一条信息高速公路，使所有美国人都能共享和使用信息资源，这就是我们现今互联网世界的雏形。



图1-9 互联网的诞生

在互联网上，我们可以方便快速地生成信息并将其复制到任何一个

地方，所有信息都是可以高效传播的，于是我们进入了一个信息爆炸的时代。为了满足人们对爆炸式信息的渴求，信息传输技术遍地开花，不断创新，比如云盘、断点续传技术等。

渐渐地，我们会发现，固然很多信息只须简单地复制粘贴就可以使用，比如视频、图片、声音等，但有些信息是无法复制的，复制后也没有意义。

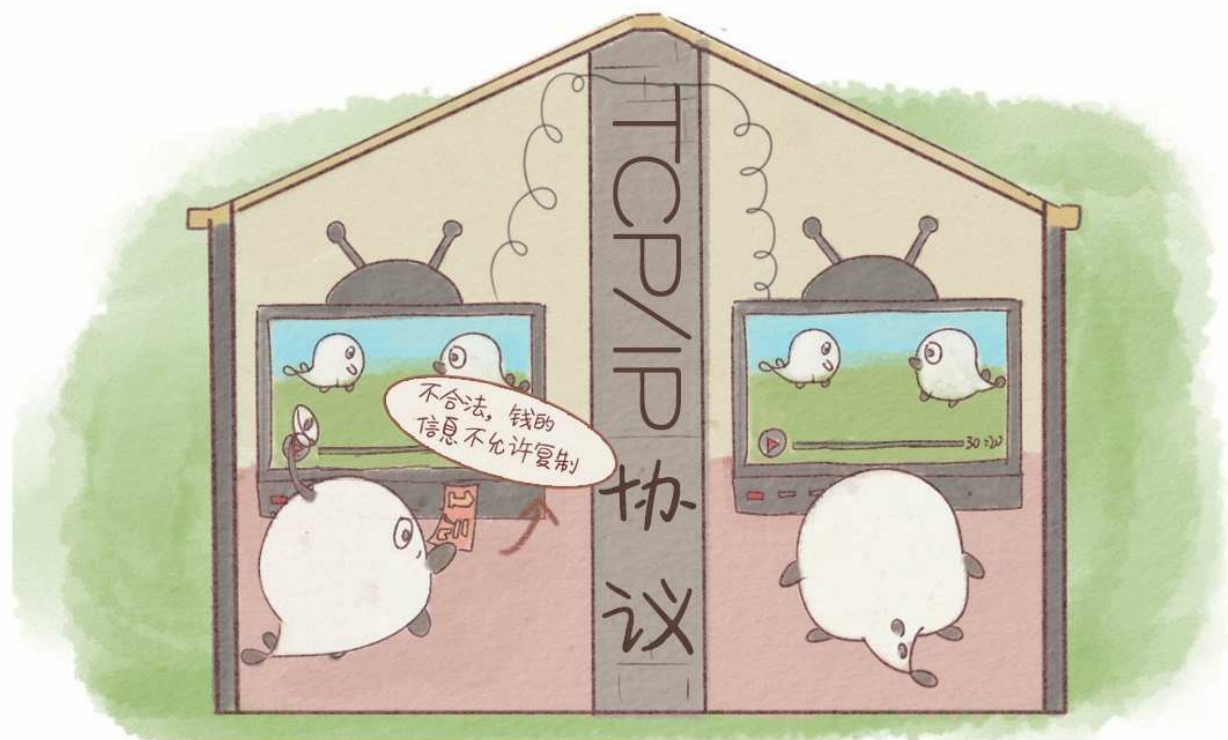


图1-10 价值转移如何解决

举个例子，我们把支付的钱直接复制给对方是不行的，而是要在付款账户上减去一些钱，在收款账户上增加一些钱，才能完成支付过程。一个视频可以被复制到另一个网站上，那么两个网站都可以看到这段视频，人们都可以分享。但一些只能转移而不能分享的有价值的信息往往需要信用背书。互联网很善于处理信息分享，却不能解决价值转移这件事。

我们来更简单地阐释一下价值转移这个概念，将某一部分价值从A地址转移到B地址，那么需要A地址精确地减少了这部分价值，而B地址精确地增加了这部分价值。价值转移涉及A和B这两个独立的参与者，那么这个操作就必须同时得到A和B的认可，而且，结果还不能受到A和B任何一方的操纵，目前的互联网协议是不支持价值转移功能的，所以，目前的价值转移往往不是直接传输，而是由一个中心化的第三方来做背书。



图1-11 中心化的第三方

现如今的中心化机构通过政府或者集团公司的背书，把所有价值转移的计算都放在一个中心服务器中进行处理，其中一定会涉及人的参与，而人的“有限理论”和“机会主义行为”往往会使整个系统变得不那么可信。那么一个最基本的问题又产生了，如何达成信用共识？

区块链技术就这样应运而生了，它可以在没有第三方信用背书的情况下，在一个开放式的平台上进行远距离的安全支付。区块链跨越多个遍布全球各地的节点，保存所有交易的历史记录。

而且，网络中所有授权的参与者都保存着一份完全相同的账本，一旦对账本进行修改，全部副本数据也将在几分钟甚至几秒钟内全部修改完毕。分布式账本中的每一笔交易都有一个独一无二的时间戳，这样可以防止重复支付的产生。

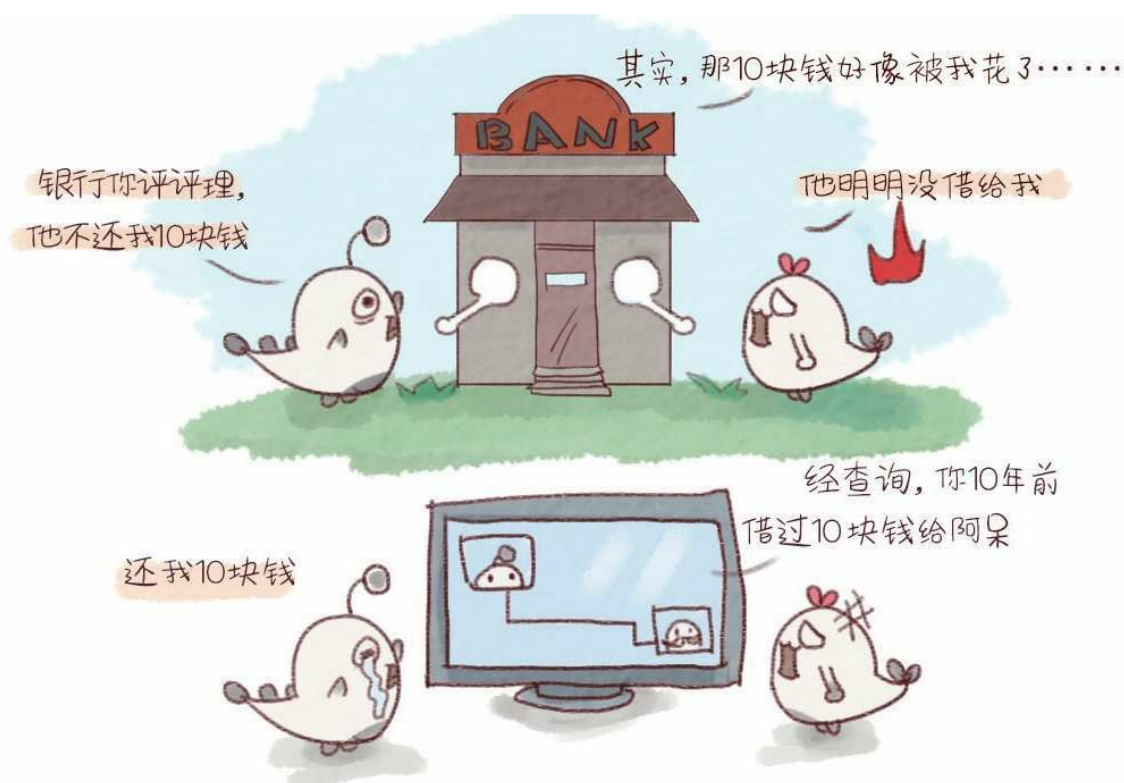


图1-12 区块链的信用共识

可以说，区块链可以构建一种纯粹的点对点的价值转移体系，在不需要各节点互信的情况下，区块链可以保证系统内数据记录的完整性和安全性，可以脱离第三方机构背书，有效地降低交易的复杂性和风险。

最后，我们不得不提一下区块链的另一个特性——可编程性，这是一个开源的技术。互联网的开放性创造了一个辉煌的互联网时代，那

么，我们是不是也可以假设，开源的区块链技术也能开拓一个新的世界呢？

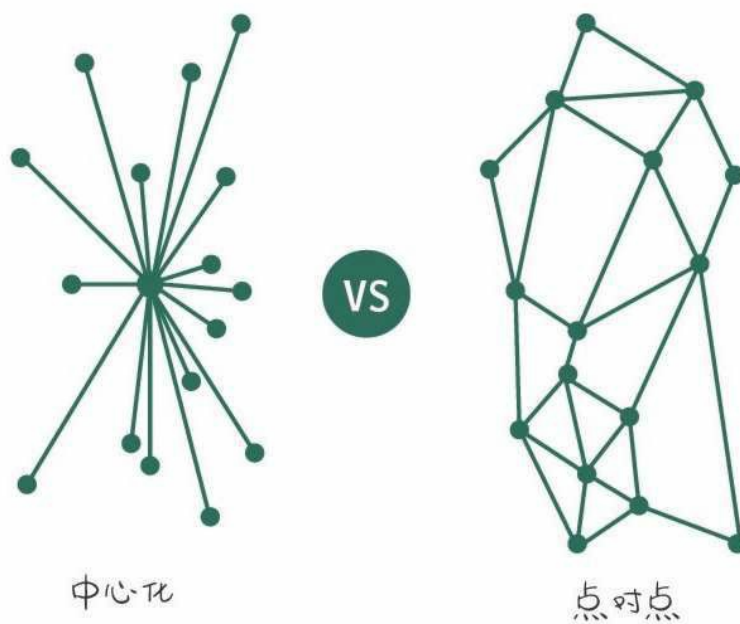


图1 - 13 中心化VS点对点结构

信用成本：你能记住多少人的脸

你有想过一个问题吗——你能记住多少人的脸？你有听过“e租宝跑路”事件吗？这些都会引入一个问题：信用共识。相信一个人需要什么成本？一旦公信力机构出现了问题，信任又将何处安放？

有一个人类学家在研究部落的时候发现，每一个部落都被控制在150人左右的范围，因为人再多一些的话，大家就记不住彼此了，记不住脸就感受不到亲近，感受不到亲近就培养不了信任，没有信任，部落之间的战斗和争端就永远不会停止。

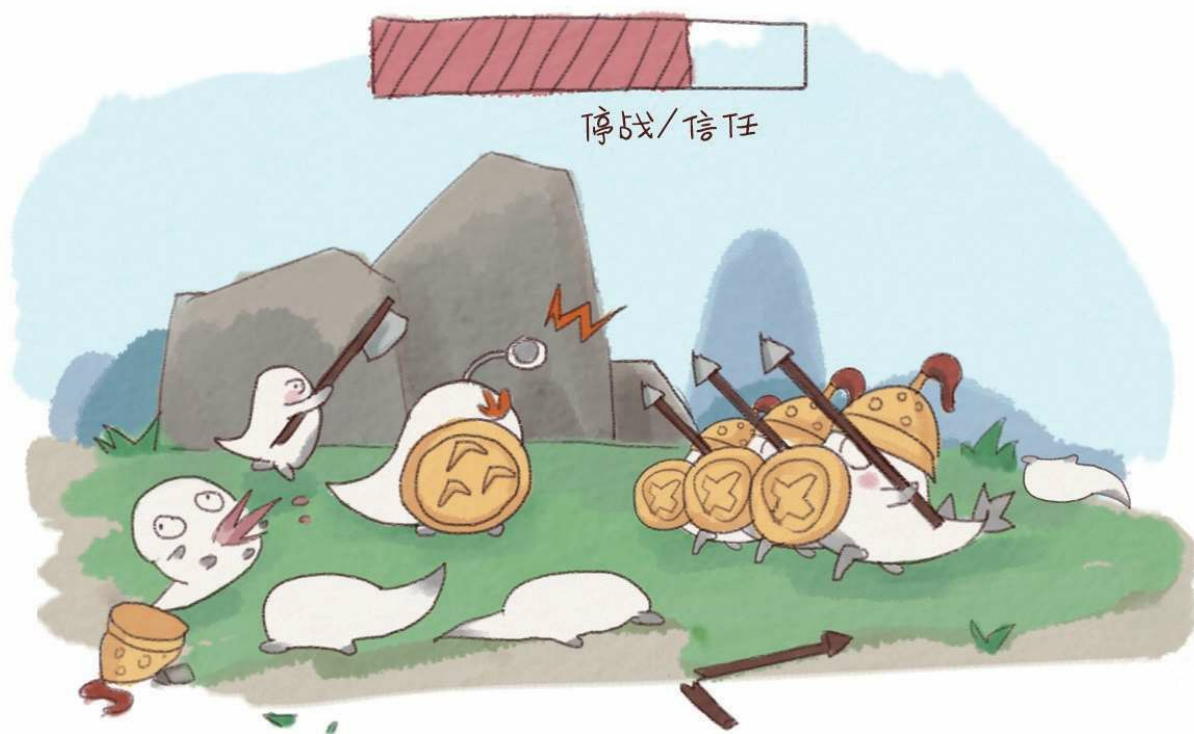


图1-14 部落时代的信任危机

在部落时代，或许只是因为人群中多看了一眼，就会被打成熊猫

眼，而到如今的互联网时代，为什么大家愿意去相信远在千里之外的一个卖衣服的商家，并且给他付款呢？因为在这个交易过程中，我们把信任托付给了国家机构或者大型企业，我们和卖衣服的人之间仍然是不信任的，但是，由于国家或大型企业的背书，我们愿意让其做个见证，这是一种比较常用的增加互信的方式。

【更多新书朋友圈免费首发，微信jrgh3w】

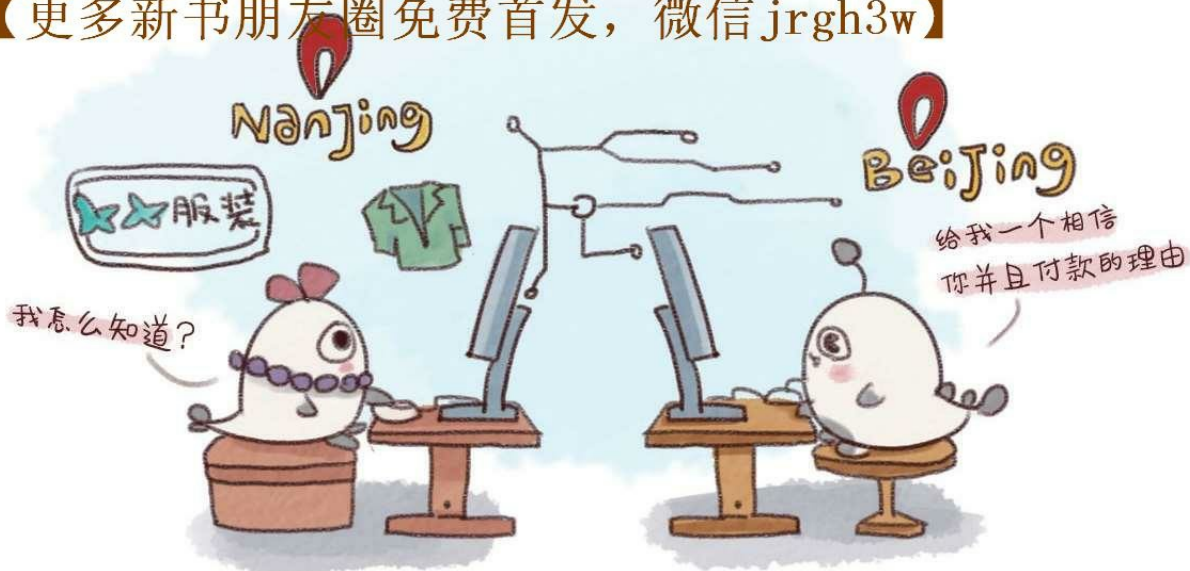


图1-15 互联网时代中心化信任

在那么多让人们增加互信的办法中，有一种拯救信任危机的利器正是区块链。区块链是比特币金融系统中的核心技术，它的实质是一个不断增长的分布式结算数据库，能完美解决信息系统中的信任危机。

它起源于下面的问题：你凭什么相信一个陌生人？别人凭什么相信你？区块链用算法证明机制来保证这份信任。借助它，整个系统中的所有节点能够在信任的环境下自动安全地交换数据。与费时费钱的其他工具技术相比，它能实时自动撮合、强制执行，而且成本很低。



图1-1 6区块链带来智能化信任

与其相信人，不如相信技术。区块链技术带来的是一种智能化信任。我们举个例子，洪都拉斯政府用区块链技术建立了一套新的房地产契约登记和交易制度，因为之前洪都拉斯一直动荡，政府工作人员偷懒，以致登记不详或记录丢失，这类纠纷在全球都很普遍。有了区块链技术的安全加密保驾护航，人们就不用再担心政府腐败会导致自己的产权被篡改了。



图1-17 政府腐败导致产权被篡改

未来，数字化的信息都可以加入区块链，只要能入链，信息产权就可以明晰，就可以设定保护条件，就能自动发起和强制实施交易合约，你也无须担心信任验证和信任的执行，因为区块链都帮你实现。

说完了信用成本的问题，我们再来看看e租宝事件，通过这个事件，我们来谈一谈公信力的问题。

2015年，有一家P2P（人人贷）公司把所有的规则都一起打破，它起于乱世，却死于疯狂的扩张和令人瞠目的犯罪手段，震惊了整个中国，这家公司的名字叫作e租宝。^[2]在被调查之前，e租宝在各大卫视黄金时间进行了大量的广告投放，相当于利用公信力对具有高风险的互联网金融产品进行背书。当一群缺乏投资知识的投资人遇到了一群没有敬畏之心的投机者，悲剧就这样产生了。



图1-18 e租宝事件

现实社会中，人与人、人与公司、公司与公司之间的交易需要公信力提供支撑。公信力意指在社会生活中，公共权力面对时间差序、公众交往以及利益交换时，所表现出的一种公平、公正、公开、人道、民主与责任的信任力。当前社会，公信力一般由政府、国家机关或政府授权的第三方组织来提供。[\[3\]](#)

区块链技术可以很好地满足公信力需求，并把公信力抽象出来作为一个独立的而不是由政府或第三方组织掌控的存在，形成政府、大众、区块链与公信力互相监督的“公信新格局”。信任是建立在区块链上的，而非由单个组织掌控，从而公信力可以被多方交叉验证与监督。

区块链使公信力独立于第三方

【更多新书朋友圈免费首发，微信jrgh3w】

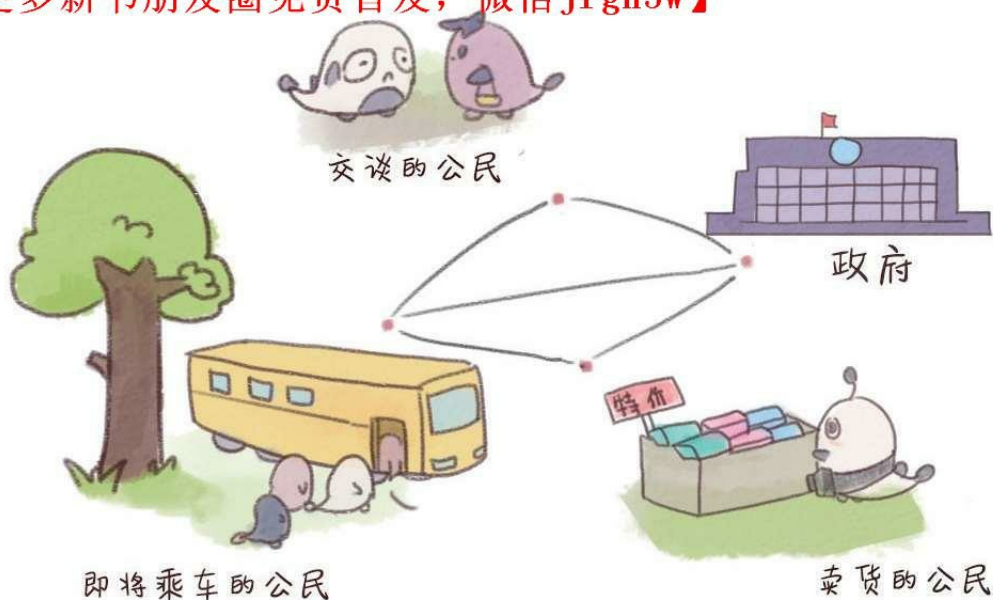


图1-19 区块链公信力

区块链公信力有什么特点呢？

1. 区块链是分布式的，区块链公信力在网络上会有许多独立的节点，每一节点都有一份备份信息。每个有授权的人都可以从任意一个节点下载全部的信息，同时，区块链公信力网络也是不可篡改的，任何节点企图更改信息都会被其他节点发现，而更改的节点不会被确认，就会立刻丧失公信力。

2. 在区块链公信力模型中，区块链不制定政策，它只是一个公证人的角色，是政府建立和执行政策的工具。区块链的作用是帮助政府更快速和准确地让政策被全民所接受与认可，同时，因为区块链是一个不变的、可以被复制的数据库，政府的政策就变得公开和透明。

从信任的角度来看，区块链实际上是用基于共识的数学方法，在机器之间建立信任并完成信用创造。基于这样的特点，其对公信力的提升

也有着开创性的意义。《经济学人》杂志这样写道：区块链是一台创造信任的机器，可以说区块链最核心的问题就是解决信用共识的问题。

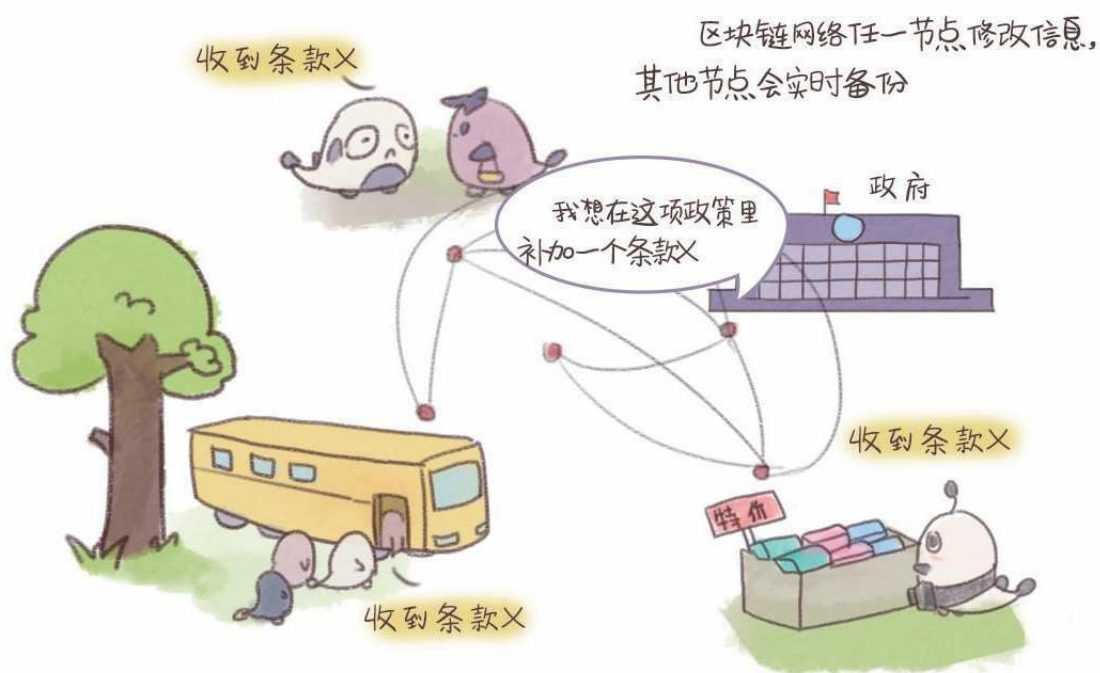


图1-20 区块链公信力场景

技术创新：从比特币到区块链

我们都知道，区块链是比特币的底层技术，可以说它是一种分布式数据存储模式，也可以说它是储存加密货币（例如比特币）的交易记录的公共账本。它的记录是加密的，被所有运行这个软件的机器所持有。

要说区块链就必然会讲到数字货币，毕竟区块链是为了满足比特币独特的需求才被创造出来的。而比特币则源于一个神秘的人物——中本聪。2008年，中本聪发表了一篇论文《比特币：一种点对点的电子现金系统》，这篇论文堪称区块链技术和加密数字货币发明的基础。



图1 - 21比特币的出现

在这篇论文中提出了比特币的几个基本原则：

1. 一个纯粹的点对点电子现金系统，使在线支付能够直接由一方发起并支付给另一人，中间不需要通过任何金融机构。
2. 不需要授信的第三方支持就能防止双重支付，点对点的网络环境是解决双重支付的一种方案。
3. 对全部交易加上时间戳，并将他们并入一个不断延展的基于哈希算法的工作量证明的链条作为交易记录。除非重新完成全部的工作量证明，形成的交易记录将不可更改。

4. 最长的链条不仅将作为被观察的事件序列的证明，而且被视为来自CPU（中央处理器）的计算能力最大的池。只要大多数CPU的计算能力不被合作攻击的节点所控制，那么就会生成最长的、长度超过攻击者的链条。

5. 这个系统本身需要的基础设施非常少，节点尽最大努力在全网传播信息即可，节点可以随时离开和重新加入网络，并将最长的工作量证明作为该节点离线期间发生的交易的证明。

看完上述的观点和逻辑，你是不是已经相信这样的理论是可行的，无须中心化的干预或者参与，只要让网络扮演信用中介的角色，就能实现有效的点对点交易。依照这样的理论，第一个比特币交易系统产生了，第一个区块（“创世区块”）产生了，第一个比特币支付的案例产生了，至今，比特币已经安稳运行了8年，没有出现过技术上的严重失误。

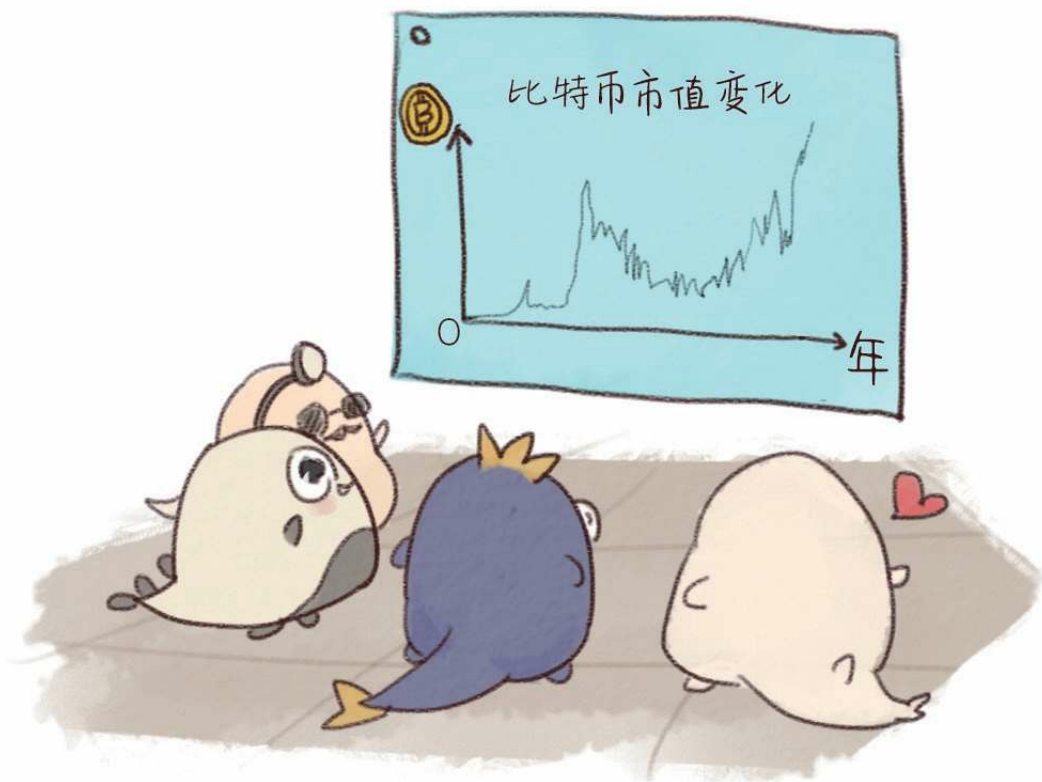


图1 - 22 比特币安稳运行8年

实际上，作为比特币的底层技术，区块链与比特币不是简单的“父子”关系，区块链也不是比特币的意外产物。区块链的产生是伴随着比特币而出现的，区块链体现了比特币的可供性，这种载体提供了一种更为广阔的交互可能性。

[1] 区块链技术在区域性股权市场的五大应用场景[EB/OL]. (2017-03-16)[2017-05-18]. <http://www.51jrit.com/news/detail/6246>.

[2] e租宝背后的互联网金融之殇[EB/OL]. [2017-05-18]. <http://weixin.niurenqushi.com/article/2016-03-07/4176154.html>.

[3] 蔡维德，罗佳。区块链所带来的公信力革命——以区块链对保险行业的影响为例[EB/OL]. (2015-12-15) [2017-05-18]. <http://www.civillaw.com.cn/zt/t/?id=29937>.

02 原理篇

信用共识带来的智能信任

今年春节回家的时候，我像往常一样应付着各种问题，诸如做什么工作的？什么时候结婚？一个月挣多少钱？但是，今年，我的答案似乎不能让他们满意，原因是当我说起我在一家区块链技术公司工作的时候，随之而来的是一个80%的人会追问的问题，什么是区块链？

我试图引用百度上的概念去解释，也试图告诉他们我们用区块链技术做了哪些厉害的事情，但是他们仍然不明白区块链是什么——不能简单点说吗？

于是，我意识到，百度上的概念以及学术杂志的解释或许不能让他们满足，于是我开始沉迷于博客、知乎，想看看大家都是如何解释区块链这个晦涩又抽象的概念。在这中间，有两篇文章对我的影响很深，一篇是知乎上的一个热门话题“如何向弱智室友解释区块链”，另一篇是博客频道用户“张童鞋”的一篇名为“区块链上的共识机制”的文章，在下面的阐述中我也部分引用了他们的观点并尝试了他们讲故事的方式。

讲一个故事，什么是区块链

区块链与骑自行车的人

2016年，包括摩根大通、花旗集团、高盛集团、纳斯达克等在内的金融巨头，都表达了对区块链技术的热衷。这些巨头们热衷的区块链技术，又被称为分布式账本，那么分布式账本究竟是什么呢？我们先从另外一件事说起。

在纳斯达克成立之前，人们用自行车驮着装满债券的包，在华尔街骑来骑去，目的就是尽快完成清算。后来业务越来越多，自行车就忙不过来了。20世纪60年代，华尔街每周只交易4天，每天4个小时，就是为了能让清算速度跟上交易量。

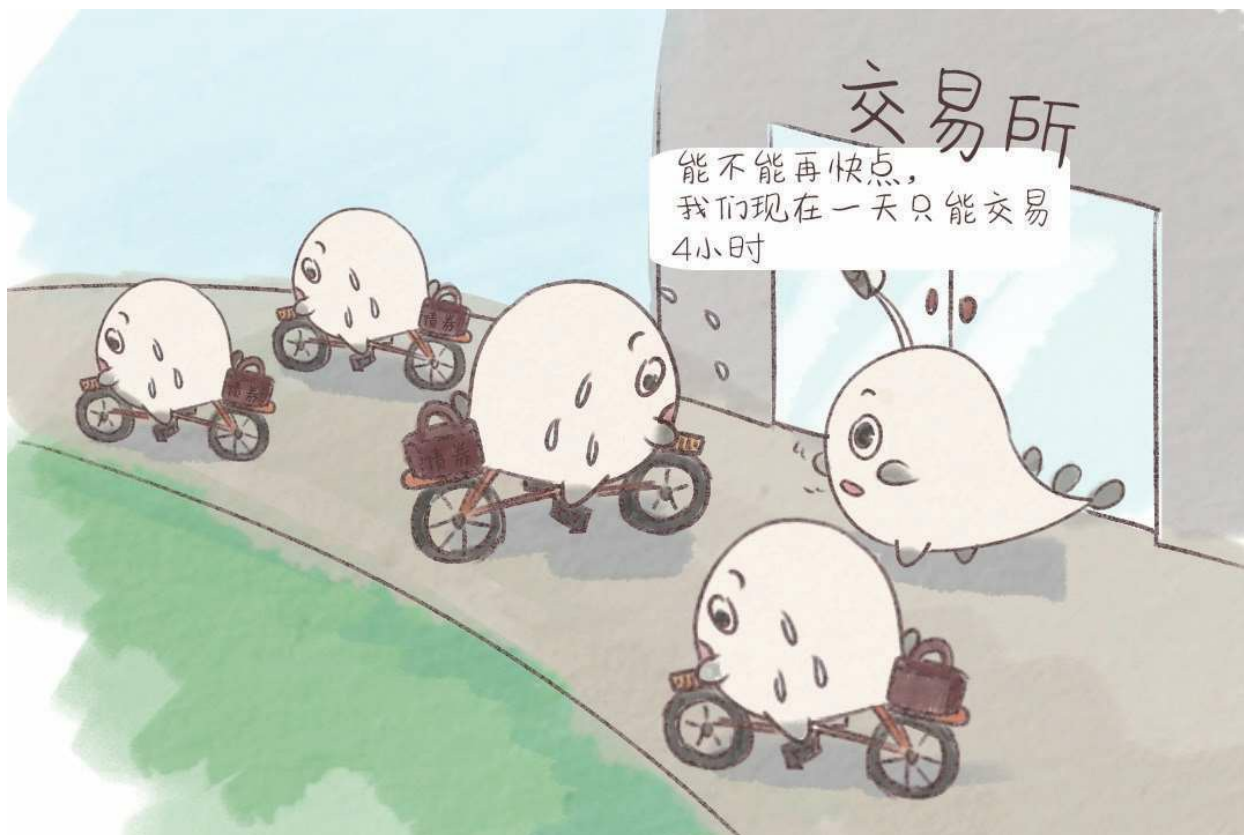


图2-1 华尔街上骑自行车的人

这样发展下来，大家觉得不行啊，自行车肯定跑不过计算机。1971年，有人就开会说，咱们想想办法吧，于是提出了DTC（美国存管信托公司）清算系统。这个系统的办法就是所有的交易都要在系统内进行，包括经纪人也要接入这个系统，现在纳斯达克还在用。

很明显，它的问题只是换了一辆可以踩油门的自行车。我们常常看到一些影视剧里，皇上、一家之主的去世导致整个国家和民族陷入混乱甚至崩溃，根本原因就在于中央集权这种系统是没办法长存的。当交易足够多、经纪人足够多的时候，我们发现，这个系统也有瘫痪甚至崩盘的危险。



图2-2 中心化的DTC清算系统

于是专家们想，自治式、分布式的系统会不会好一点呢？答案是肯定的。区块链就是一个分布式的账本，每个节点都可以显示总账，然后维护总账，而且不能篡改账本，除非你控制了超过51%的节点，但这是不可能的。

再简单一点，假如你们家里有个账本，让你来记账。在以前，就是爸爸妈妈把工资交给你，让你记到账本上——想想还是有点小激动的。中间万一你贪吃，想买点好吃的，可能账本上的记录会少十几块，然后你想买个手机，账本上就少记录几千块。这只是举一个例子，我相信小时候大家都想从爸爸妈妈的口袋里拿点钱来花。

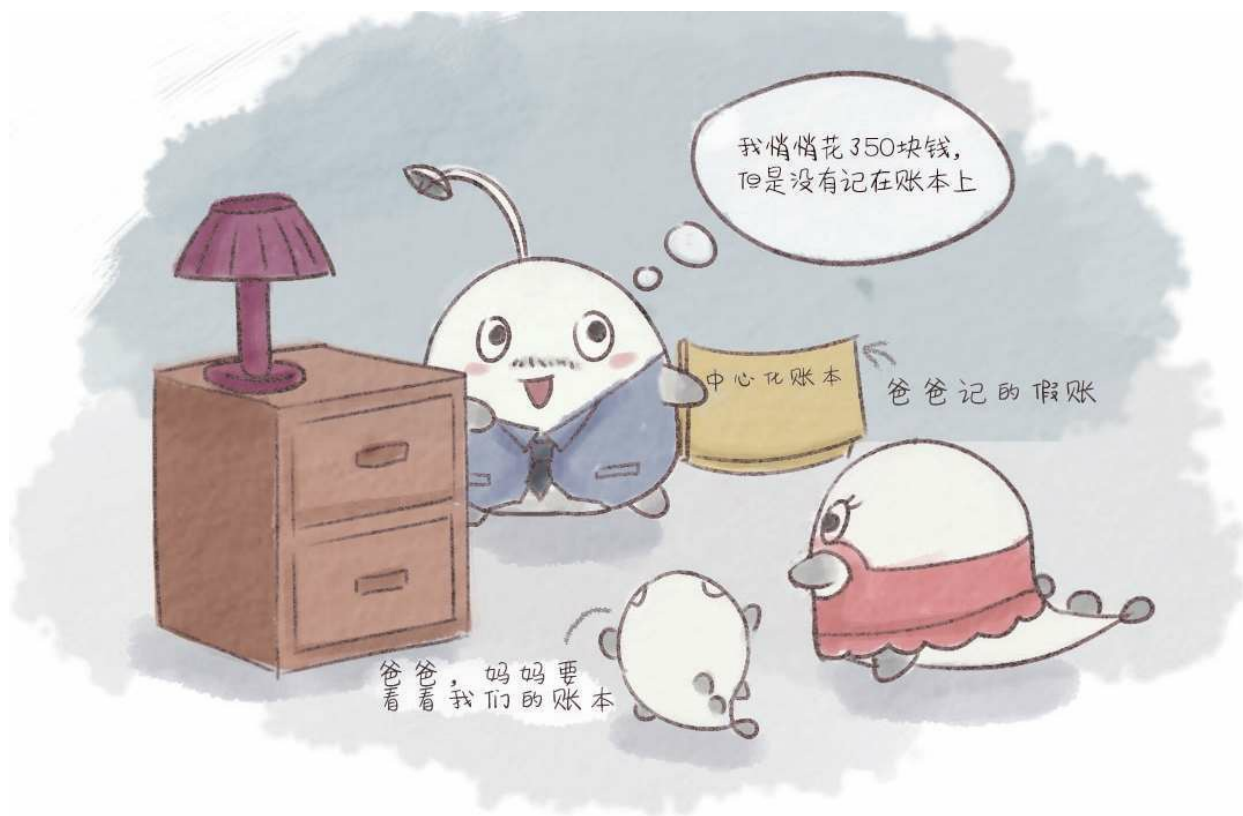


图2-3 中心化的家庭账本

但有了分布式账本后，这些问题就不会有了，因为你在记账，你爸爸也在记账，你妈妈也在记账，他们都能看到总账，你不能改，爸爸妈妈也不能改，这样想买烟抽的爸爸和想贪吃的你都没办法啦。

区块链本质上是一个去中心化的分布式账本，其本身是一系列使用密码学而产生的互相关联的数据块，每一个数据块中包含了多条经比特币的网络交易有效确认的信息。



图2-4分布式家庭账本

中心化与去中心化

前面我们说到了区块链的本质是一个去中心化的分布式账本，那么，所谓的中心化又是什么呢？我们首先思考这样一个问题，你要在网上买一本书，交易流程是什么？

第一步：你下单之后把钱打给了支付宝。

第二步：支付宝收款后通知卖家可以发货了。

第三步：卖家收到通知后给你发货。

第四步：你收到货之后很满意，于是确认收货。

第五步：支付宝收到了你的通知并打钱给卖家。

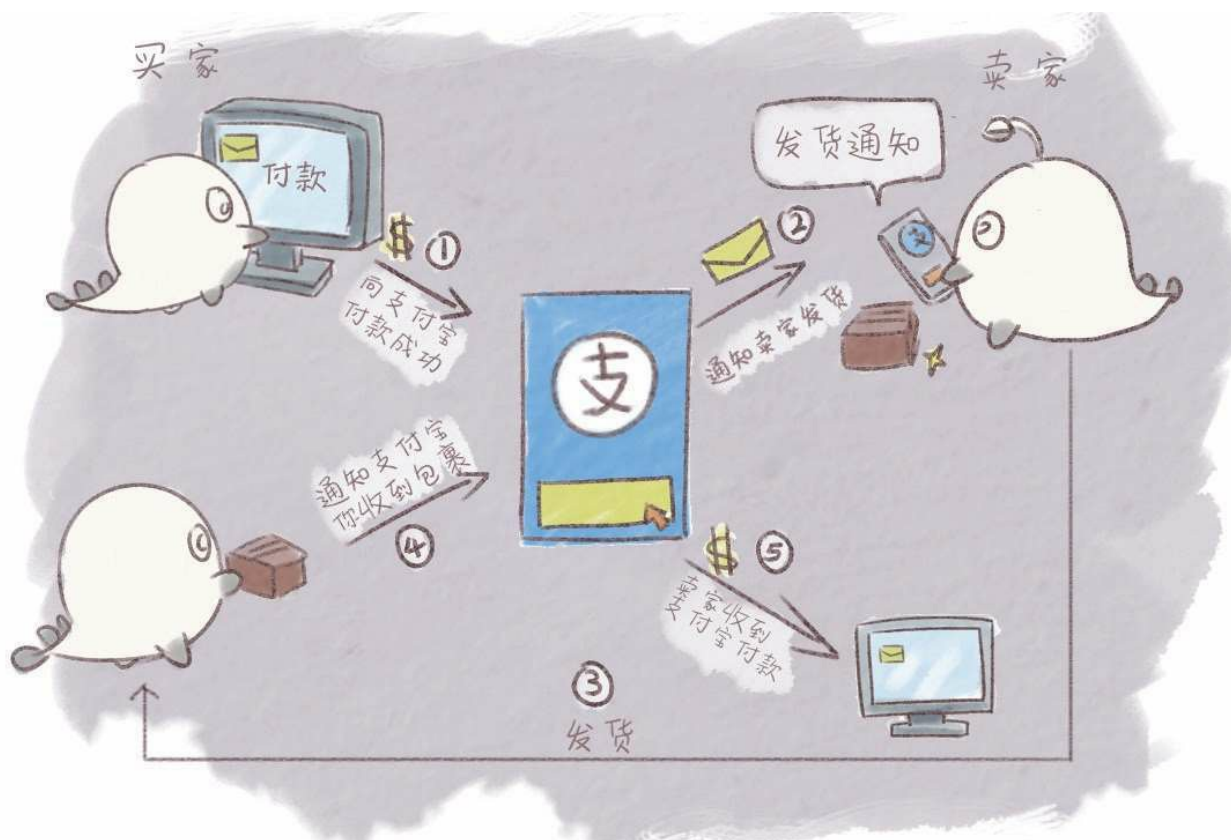


图2-5 中心化的交易流程

我们可以看出，在这个过程中，虽然你是在和卖家交易，但是整个交易都是围绕支付宝展开。因此，如果支付宝系统出了问题，比如天上降下来一块陨石，把支付宝的服务器全砸了，或者由于全球经济危机支付宝倒闭了，无奈的支付宝只好淡然地表示不存在这笔交易，那么这笔交易就会以失败告终，到时候买家卖家就会纠缠不清，双方无法自证。

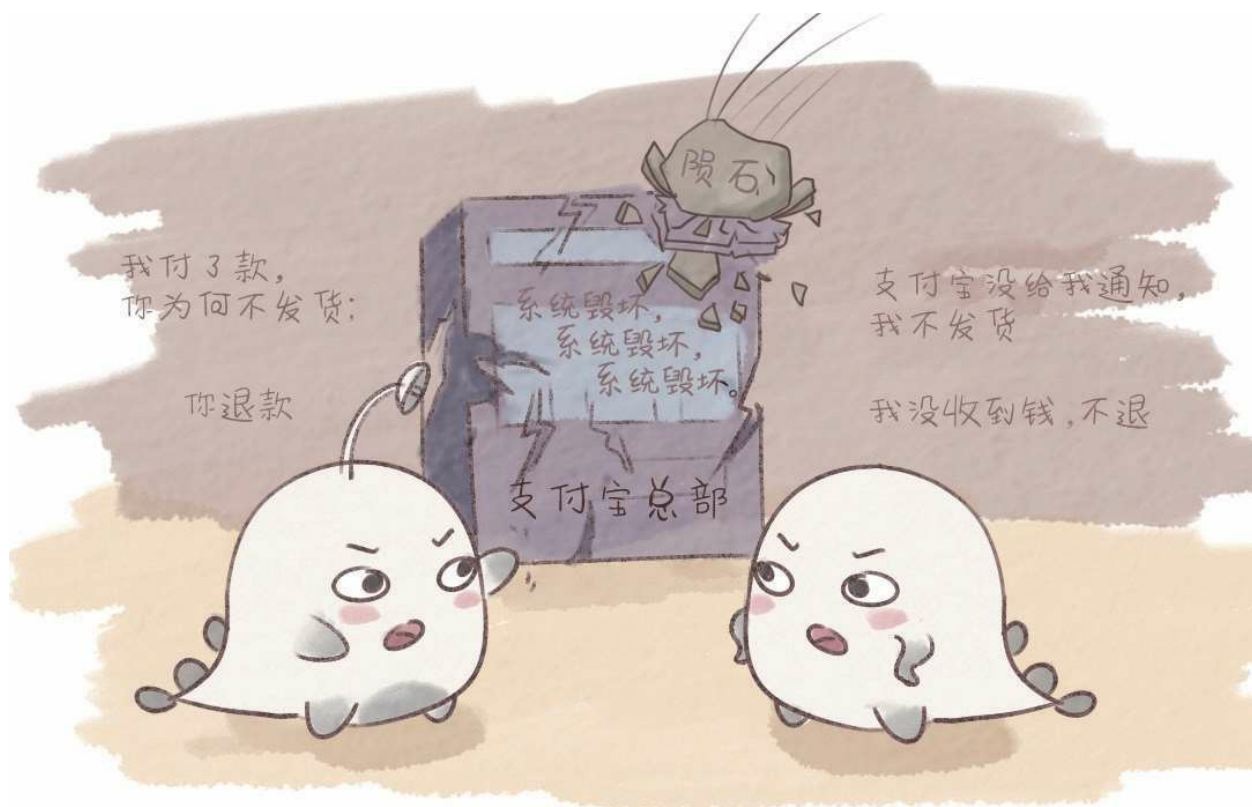


图2-6 中心节点毁坏会导致交易失败

模拟一个区块链小城市

为了说明去中心化的区块链是如何运行的，我们先把整个去中心化的分布式结构简化为一个极端的情况来探究。我们假设有一个去中心化的小城市，在这个城市里有5个可爱活泼的小伙伴，他们互相借钱的时候，是这么干的：

假设B向A借了1块钱，这个时候，城市里的人怎么办呢？A在人群中大喊：“我是A，我借给了B1块钱！”B也在人群中大喊：“我是B，A借给了我1块钱！”

此时城市里的其他人C、D、E都听到了这些消息，他们拿出了手中的小账本并默默记下：“某年某月某日，A借给了B1块钱。”



图2-7 去中心化城市的记账

当我们把一个去中心化的模型极度简化之后，我们就会发现，在这个只有5个人的城市中，已经建立了一个去中心化的系统，这个系统不需要银行，也不需要支付宝。这个模型不需要信任关系，也不需要一个拥有公信力的组织。当分布式结构中的每个人都记账的时候，篡改账本是不可行的。比如B突然不认账了：“我不欠A的1块钱！”这个时候，人民群众C或D或E就会站出来说：“不对，我的账本上明明记录了你在某年某月某日向A借了1块钱，并且没有查到你还款的记录。”



图2-8 去中心化账本无法篡改

说到这里，你有没有发现一个问题，在这个模型中，所谓的1块钱根本不重要，也没有人在意，“1块钱”已经变成了一个变量，它可以被替换成任何概念，只要大家承认这是一个有价值的东西即可。

比如A在这个城市中大喊一声：“我创造了一个巴拉拉能量！”城市中的其他人都听见了，于是大家纷纷在自己的小本子上记下“某人有一个巴拉拉能量”，大家甚至不用知道巴拉拉能量是什么，A竟然真的有了一个巴拉拉能量。之后呢？A还能干什么呢？A可以再大喊一声：“我给B一个巴拉拉能量。”

【更多新书朋友圈免费首发，微信jrgh3w】



图2-9 巴拉拉能量的流通

只要城市中的B、C、D、E，即城市里的所有人都承认了这个交易，那么这个交易就真的成立了，虽然现实生活中并没有巴拉拉能量。

小城市里的几个问题

当然，区块链的世界不会这么简单，它还有其他的规则来相互制约，我们先来解决下面这几个问题：

问题一：凭什么帮你记账？

凭什么你对着天空大喊一声，别人就要帮你记账，别人的时间不要钱吗？别人的小本子不要钱吗？于是，为了让大家都帮我记账，我增加

了一条新的规则，我决定给第一个听到我喊话并且将其记录在小本子上的人奖励。奖励机制也很简单，第一个听到我喊话并记录下来的人，可以得到一个巴拉拉能量的奖励。

这个巴拉拉能量不是白给的，是对你劳动的报酬，就像打工可以挣钱一样，你帮我记账，整个系统都会给你报酬。你要做的事情，有这样几点：首先，你要抢在所有人之前听到了我的喊话并记在了自己的小本子上；记录之后，你还要马上告诉整个城市里的人——这句话我记录完了，你们再记录也没有用了，别人就会放弃这笔赚钱的生意；与此同时，你还要做一件事，就是给自己的记录加一个独一无二的编号，然后把记录和编号一起喊出来，于是，下一个人再记录的时候，就会带着这个记录和独一无二的编号继续下去。



图2-10 记账获得奖励

在这条新的规则开始实行之后，一定会有这样一些人，他们为了得

到巴拉拉能量，开始屏气监听周围发出的各种声音，只为了能在第一时间记下一条新的记录。

这个时候，对区块链有所了解的读者是不是想到了这样的名词——“比特币挖矿”。没错，这就是比特币挖矿的简单说明。

关于比特币挖矿的话题，知乎用户“玲珑邪僧”的一篇文章举过一个更生动的例子，大致是这样的：单身男士们要找女朋友，“国民岳母”说，我有好多肤白貌美、乖巧可爱的女儿，这样吧，我给你们出一个旷世难题，解出一个就给你们其中一个姑娘的微信号。[\[1\]](#)

于是，单身男士们疯狂竞争，想破脑袋去解这道旷世难题。只要其中一位单身男士解出一道题，就立马得意扬扬地昭告天下，示威全部单身男士，这个姑娘的微信号是我的啦，先到先得，你们放弃吧。其他单身男士虽然已经算到一半了，但是没有办法，速度不够快啊，只好立马去解下一道题。



图2-11 “国民岳母”的旷世难题

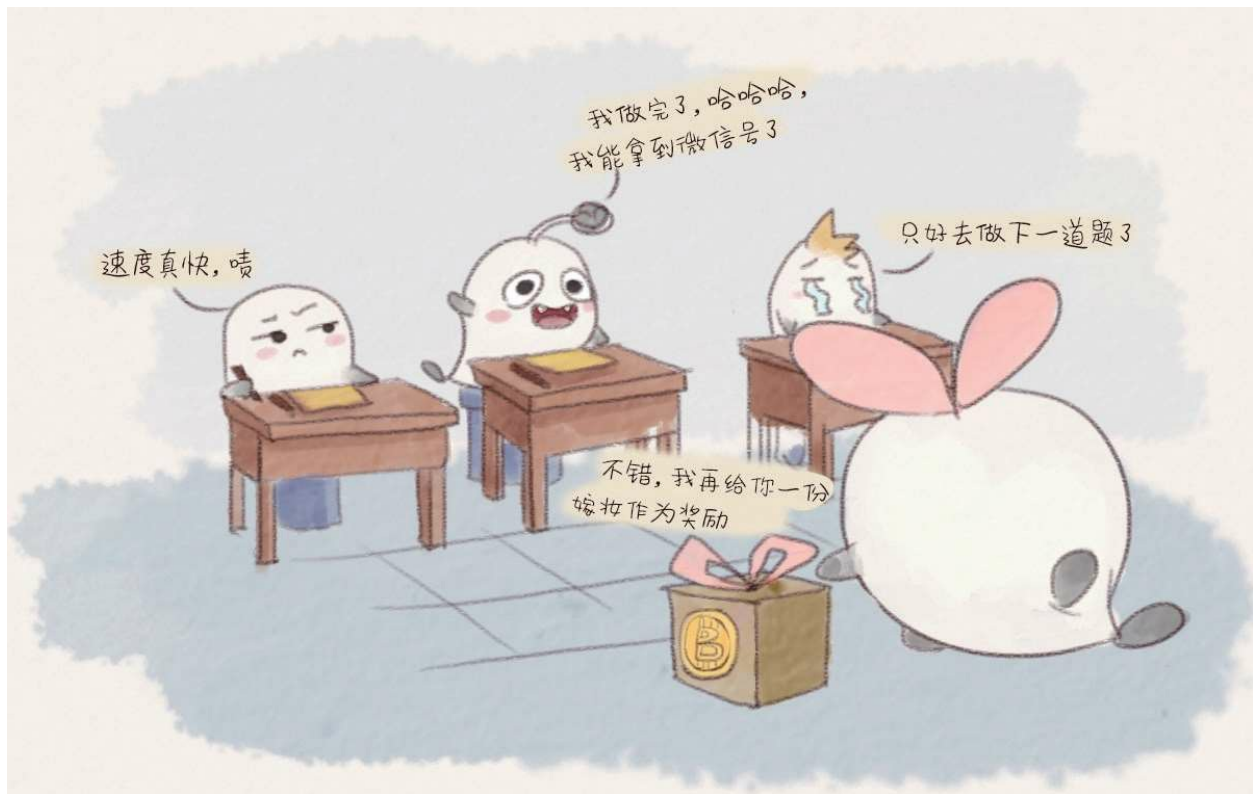


图2-12 解出难题获得奖励

同时，首个成功破解旷世难题的幸运的单身男士不仅不用付一二十万元的彩礼，被其才华征服的“国民岳母”还会给这位单身男士一笔巨额财产做嫁妆，也就是比特币挖矿中的比特币奖励。

问题二：分叉问题听谁的？

在这一段的论述中，我们引用了知乎用户“汪乐-LaiW3n”的说法。在这个广阔的小城市里，一定还会存在这样的问题，B和C几乎同时记录完了，于是同时向天空大喊了一声，“这个编号89757的巴拉拉能量归我了”。但是，由于这个城市太广阔了，有的人会认为这个编号89757的巴拉拉能量归B，也有的人认为这个编号89757的巴拉拉能量归C，但是编号89757的巴拉拉能量只有一个啊，只有一个人能得到，怎么办呢？一人一半？当然是不可能的，这个时候我们会采用更原始简单的规则来

解决，谁长听谁的。

在不加任何限制条件的情况下，这件事件会发展成这样：一部分人认为这句话是B说的，在听到这句话之后开始记账，之后他们所做的所有事情都是基于B有了编号89757的巴拉拉能量这个事实，并且随着这个信息一次次地传下去，这条信息链会越来越长；而另外一群认为C先说这句话的人，也会按照这样的趋势发展。



图2-13 分叉问题听谁的?

这下事情严重了，原本是一条唯一的、编号顺序严谨的总信息链，在B和C喊出“这个编号89757的巴拉拉能量归我了”这句话之后，硬生生地分叉了！这还得了，要是这种情况延续下去，每个人手里的账本都变得不一样了，而且根本没法确定哪个是真的！

为了解决这个问题，小城市又追加了新的区块链规则，记录的时候必须顶格写，而且要保证，中心在离田字格上边缘0.897 57毫米的位置

上，于是，每个人写字的时候都要拿刻度尺量好之后再写，这非常困难，每个人的记录需要5分钟才能完成，因此，写这句话所用的时间变得不同了。于是，只要有人高喊“我写完了！那句话是某某某写的”，其他正在写这句话的人便会停笔，然后在小本子上重新开始写“那句话是某某某写的，上一句的编号是xxx”。

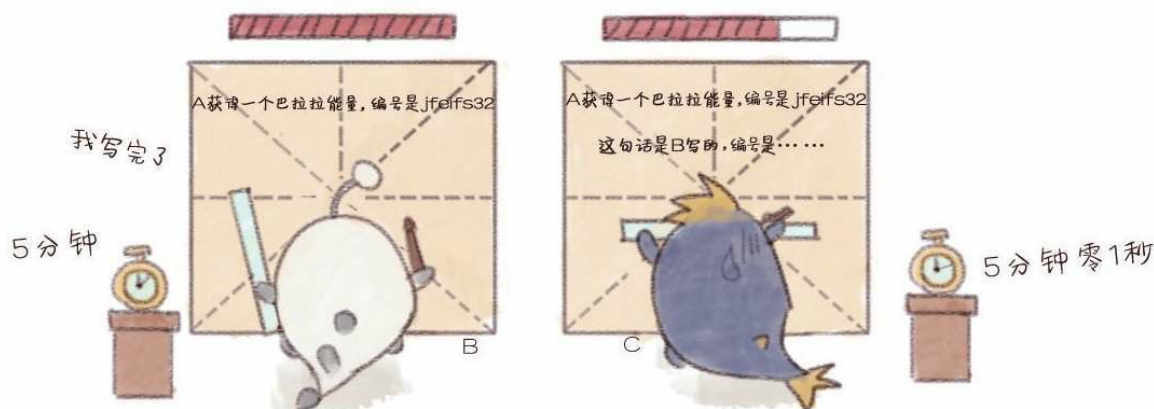


图2-14每次记账的规则都很复杂

问题三：双花问题

双花问题是指一笔数字现金在交易中被重复使用的现象。如果我同时向B和C都喊了一句，我给你一个巴拉拉能量，怎么办呢？巴拉拉能量只有一个，如何保证一个巴拉拉能量在实际的交易中只被支付了一次呢？

我们以比特币为例，中本聪在《比特币白皮书》第五小节中是这样说的，运行比特币网络的步骤如下：[\[2\]](#)

1. 新的交易向全网进行广播；
2. 每一个节点都将收到的交易信息纳入一个区块中；

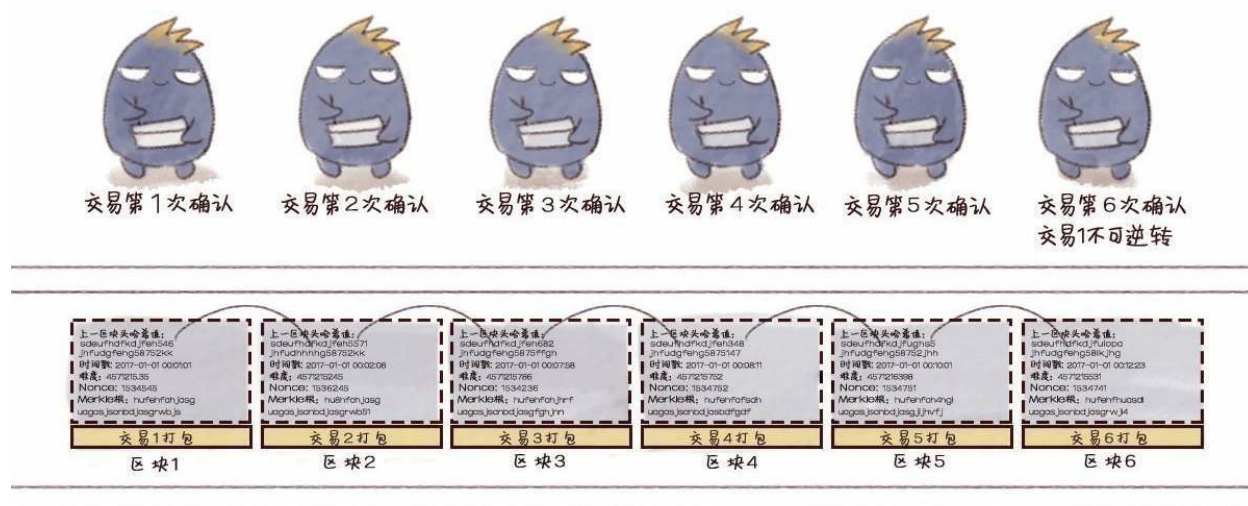
3. 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

4. 当一个节点找到了一个工作量证明，它就向全网进行广播；

5. 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；

6. 其他节点表示他们接受该区块，而接受的方法则是跟随在该区块的末尾，制造新的区块以延长该链条，并将该区块的随机散列值视为新区块的随机散列值。

也就是说，交易发生的一刻起，比特币的交易数据就被盖上了时间戳；而当这笔交易数据被打包到一个区块中后，就算完成了一次确认；在连续进行6次确认之后，这笔交易就不可逆转了；在比特币中，每一次确认都需要“解决一个复杂的难题”，也就是说每一次确认都需要一定的时间。



6次确认完成，不可逆转

图2 - 15 6次确认后不可逆转

在这种情况下，当我试图于把一笔资金进行两次支付交易的时候，因为确认时间较长，后一笔交易想要与前一笔交易同时得到确认几乎是不可能的，而这笔资金在第一次交易确认有效后，第二次交易时就无法得到确认。区块链的全网记账需要在整个网络中达成共识，双花问题是无法产生的。

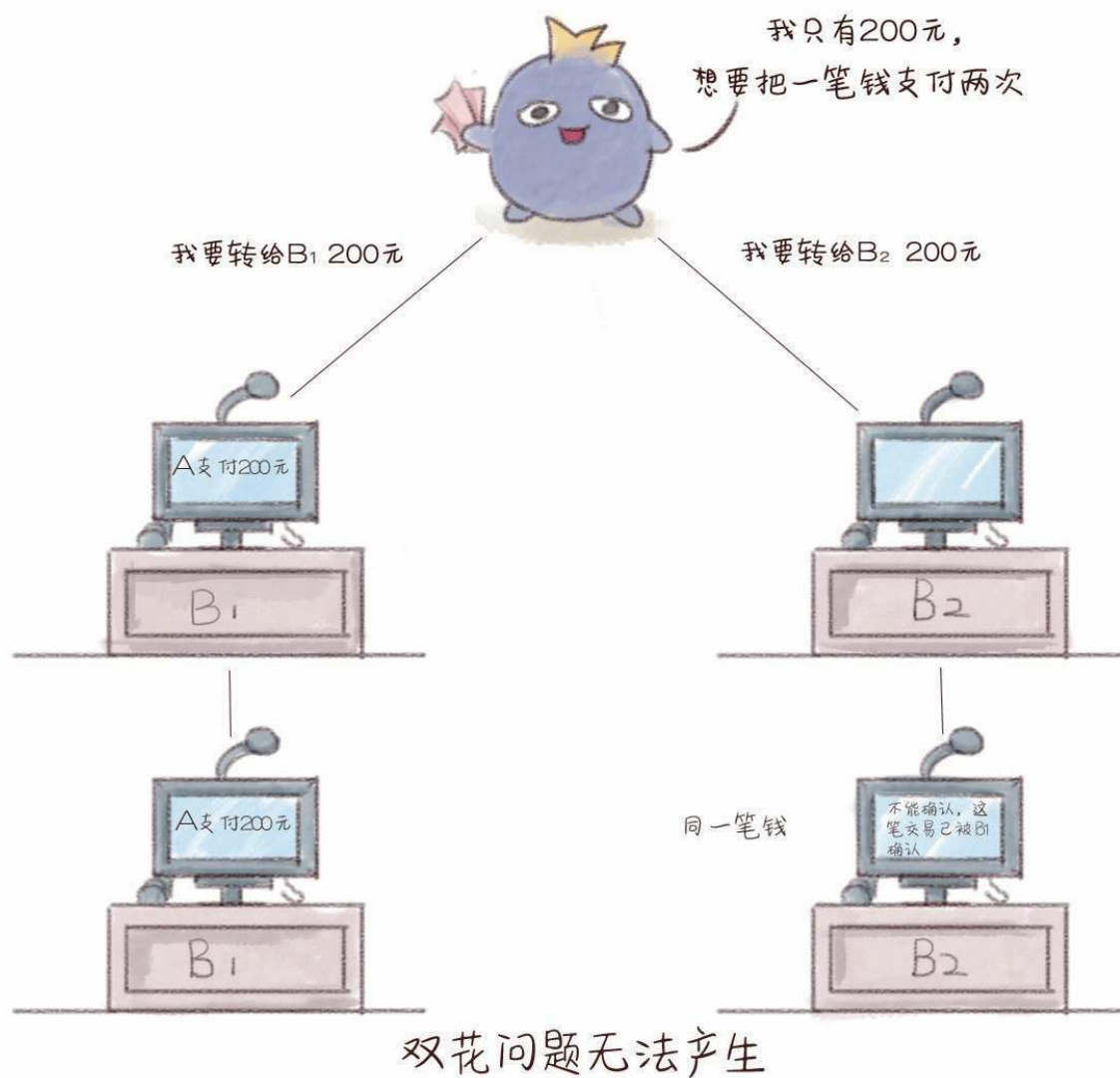


图2-16 双花问题无法产生

讲一下原理，区块链如何运作

区块链的核心概念

在讲解区块链的工作原理之前，我们先将区块链中涉及的几个核心概念做一个简单的阐述。

一、区块

区块作为区块链的基本结构单元，由包含元数据的区块头和包含交易数据的区块主体构成。

区块头包含三组元数据：

1. 用于连接前面的区块、索引自父区块哈希值的数据；
2. 挖矿难度、Nonce（随机数，用于工作量证明算法的计数器）、时间戳；
3. 能够总结并快速归纳校验区块中所有交易数据的Merkle（默克尔）树根数据。



图2-17 区块头的结构

区块链系统大约每10分钟会创建一个区块，其中包含了这段时间里全网范围内发生的所有交易。每个区块中也包含了前一个区块的ID（识别码），这使得每个区块都能找到其前一个节点，这样一直倒推就形成了一条完整的交易链条。从诞生之初到运行至今，全网随之形成了一条唯一的主区块链。[\[3\]](#)

二、哈希算法

哈希算法是区块链中保证交易信息不被篡改的单向密码机制。哈希算法接收一段明文后，以一种不可逆的方式将其转化为一段长度较短、位数固定的散列数据。

它有两个特点：

1. 加密过程不可逆，意味着我们无法通过输出的散列数据倒推原本的明文是什么；

2. 输入的明文与输出的散列数据一一对应，任何一个输入信息的变化，都必将导致最终输出的散列数据的变化。

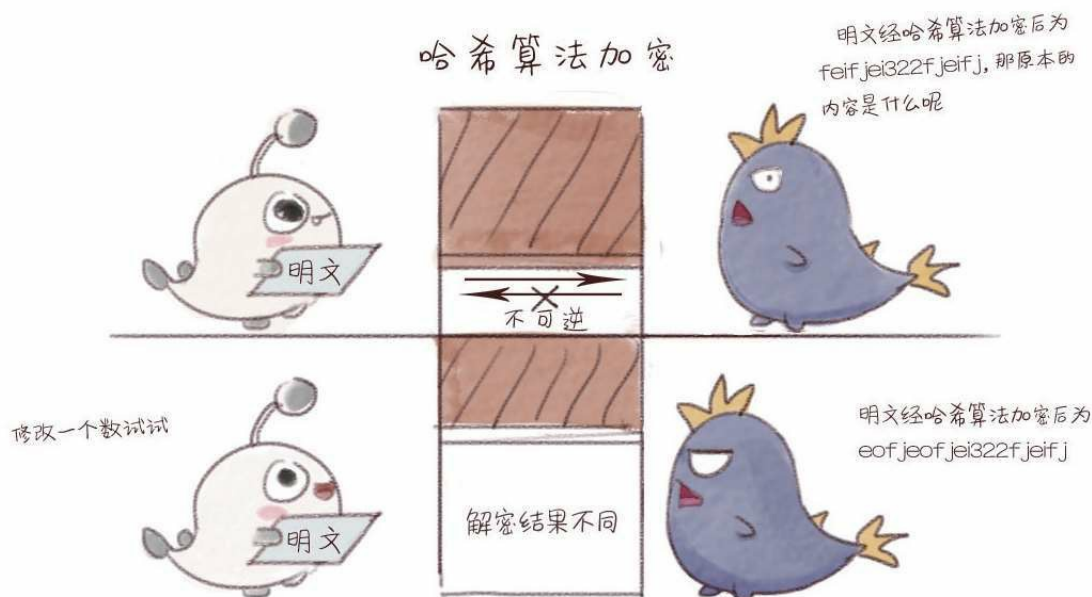


图2-18 哈希算法的两个特点

在区块链中，通常使用SHA-256（安全散列算法）进行区块加密，这种算法的输入长度为256位，输出的是一串长度为32字节的随机散列数据。[\[4\]](#)区块链通过哈希算法对一个交易区块中的交易信息进行加密，并把信息压缩成由一串数字和字母组成的散列字符串。区块链的哈希值能够唯一而准确地标识一个区块，区块链中任意节点通过简单的哈希计算都可以获得这个区块的哈希值，计算出的哈希值没有变化也就意味着区块中的信息没有被篡改。

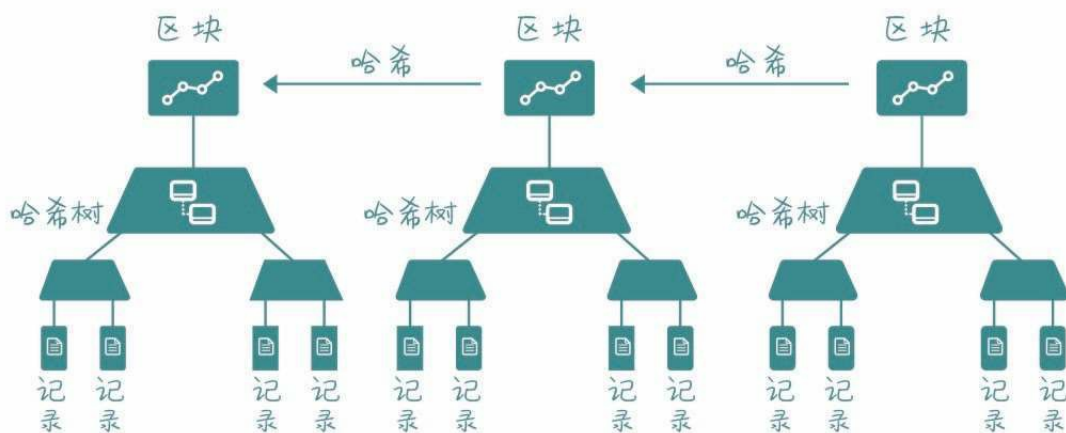


图2 - 19 区块链中的哈希算法

三、公钥和私钥

在区块链的话题中，我们还经常听到这样的词汇——公钥和私钥。这就是俗称的不对称加密方式，是对以前的对称加密方式（使用用户名与密码）的提高。

我们用电子邮件加密的模型来简单介绍一下：公钥就是给大家用的，你可以通过电子邮件发布，可以通过网站让别人下载，公钥其实是用来加密/验章的。私钥就是自己的，必须非常小心保存，最好加上密码，私钥用来解密/签章，私钥由个人拥有。[\[5\]](#)

在比特币的系统中，私钥本质上是32个字节组成的数组，公钥和地址的生成都依赖私钥，有了私钥就能生成公钥和地址，就能够花费对应地址上面的比特币。私钥花费比特币的方式就是对这个私钥所对应的未花费的交易进行签名。

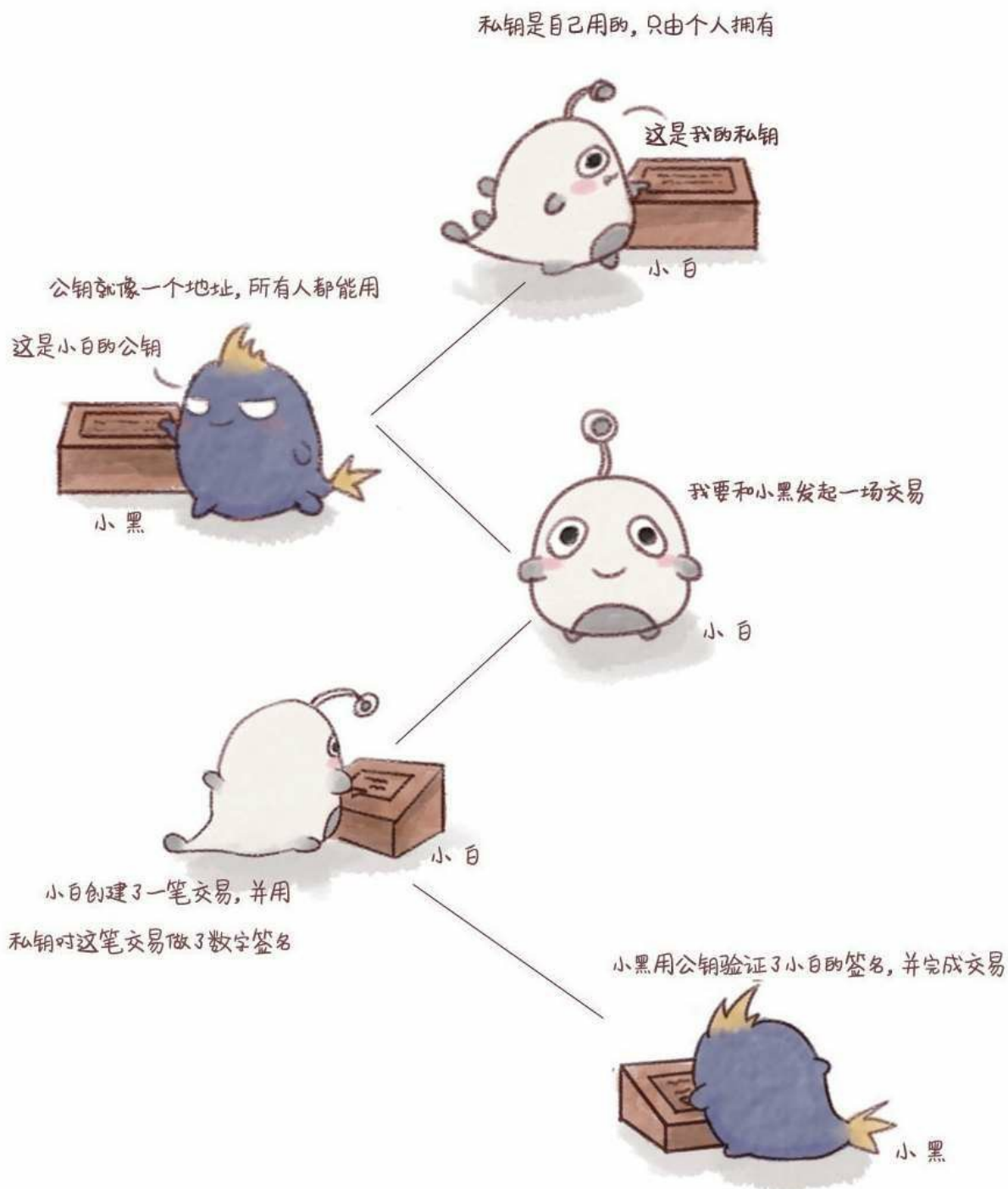


图2-20 区块链中的公钥和私钥

在区块链中, 使用公钥和私钥来标识身份, 我们假设区块链中有两个人, 分别为小白和小黑, 小白想向小黑证明自己是真实的小白, 那么

小白只需要使用私钥对文件进行签名并发送给小黑，小黑使用小白的公钥对文件进行签名验证，如果验证成功，那么就证明这个文件一定是小白用私钥加密过的。由于小白的私钥只有小白才能持有，那么，就可以验证小白确实是小白。

在区块链系统中，公钥和私钥还可以保证分布式网络点对点信息传递的安全。在区块链信息传递中，信息传递双方的公钥和私钥的加密与解密往往是不成对出现的。

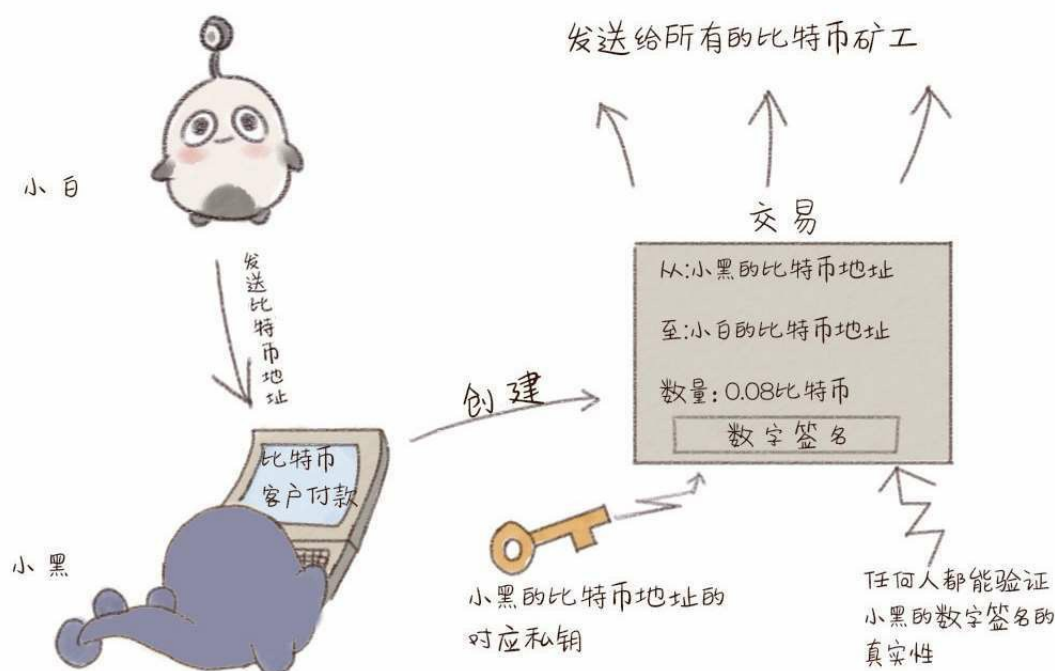


图2 - 21使用公钥和私钥完成一笔交易

信息发送者：用私钥对信息进行签名，使用信息接收方的公钥对信息加密。

信息接收方：用信息发送者的公钥验证信息发送者的身份，使用私钥对加密信息解密。

四、时间戳

区块链中的时间戳从区块生成的一刻起就存在于区块之中，它对应的是每一次交易记录的认证，证明交易记录的真实性。

时间戳是直接写在区块链中的，而区块链中已经生成的区块不可篡改，因为一旦篡改，生成的哈希值就会变化，从而变成一个无效的数据。每一个时间戳会将前一个时间戳也纳入其随机哈希值中，这一过程不断重复，依次相连，最后会生成一个完整的链条。

每个加盖时间戳生成的区块都独一无二



图2-22 区块链中的时间戳

五、Merkle树结构

区块链利用Merkle树的数据结构存放所有叶子节点的值，并以此为基础生成一个统一的哈希值。Merkle树的叶子节点存储的是数据信息的哈希值，非叶子的节点存储的是对其下面所有叶子节点的组合进行哈希计算后得出的哈希值。[\[6\]](#)

同样地，区块中任意一个数据的变更都会导致Merkle树结构发生变

化，在交易信息验证比对的过程中，Merkle树结构能够大大减少数据的计算量，毕竟，我们只需验证Merkle树结构生成的统一哈希值就可以了。

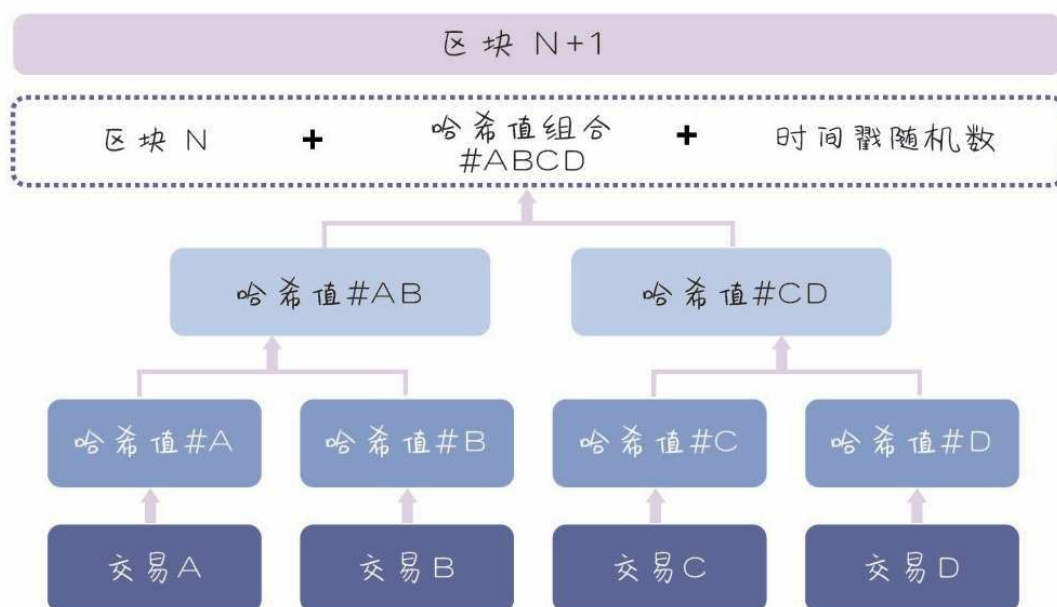


图2 - 23 区块链中的Merkle树结构

从比特币病毒谈起

前文我们说到了区块链中的几个核心概念和定义，那么，区块链究竟是如何运行的呢？要解决这个问题，我们就不得不先从比特币开始聊起。说起比特币，许多人的第一反应就是比特币病毒。下面我们就从比特币病毒这一事件引入，聊一聊比特币究竟是什么，有哪些特性。

叙述一下全世界都知道的事

还记得被比特币支配的恐惧吗？

那一天，早上醒来，你发现屏幕上弹出一个丑陋的红框框。

你异常激动，终于不用写论文了。

恭喜你获得了一个不写论文的正当理由



图2-24 比特币病毒入侵

2017年5月12日，网上发生了一件微小的事情，众多学校、医院的文档都陆续被一个叫“永恒之蓝”（WannaCry）的勒索蠕虫病毒锁住了：想看资料，可以；交钱，也不需要太多，300个比特币就行。有人一看瞬间觉得，只用300个，这么少。其实，一个比特币的价格在中国差不多等于一万元，这还是因为中国的比特币平台正处于监管期不能提现，国外的价格就更高了。当然，对于个人用户来说，是不需要给这么多钱的，毕竟并不是谁都有300多万元的。

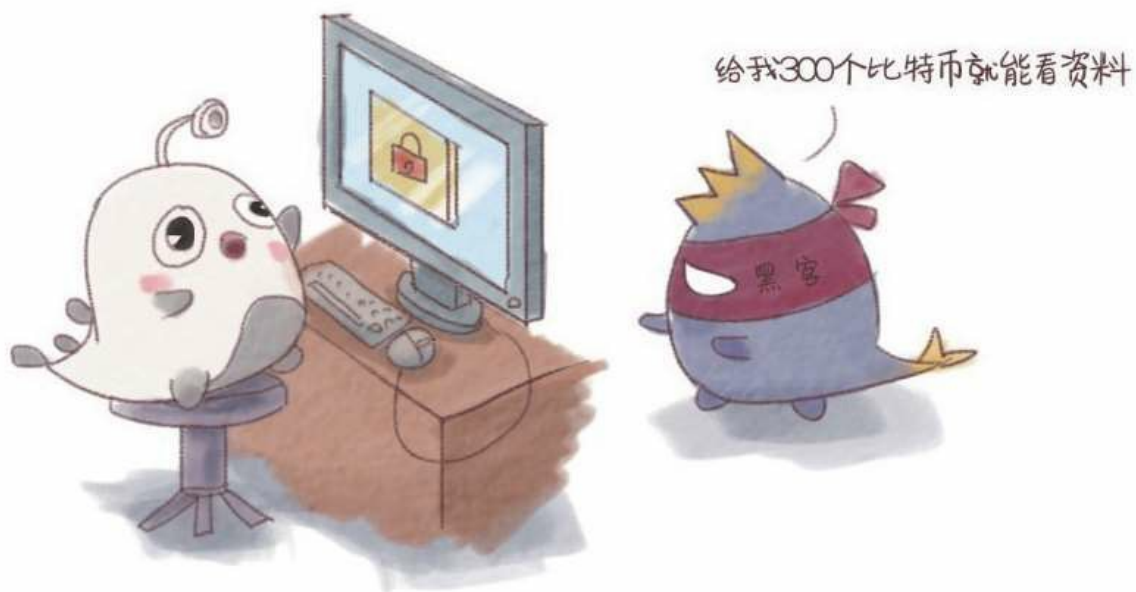


图2-25需要比特币赎金才能解锁

黑客想让大家用比特币支付，不过这事本身和比特币还真没什么太大关系。比特币就是一种币，本来安静地在旁边躺着，早上醒来却发现自己上头条了。截至2017年5月16日，已经有150多个国家的30多万用户受到“迫害”了，而且，有消息显示，“永恒之蓝”病毒已经升级为2.0版本了，新版本病毒不受域名限制，传播性更高。



图2-26 “永恒之蓝”

那么，这个比特币病毒究竟是什么东西呢？它可以被视为由两种东西混合开发出来的神奇病毒——加密算法勒索病毒和“永恒之蓝”黑客工具。“永恒之蓝”黑客工具负责开道，不需要点击直接入侵别人的电脑，然后加密算法勒索病毒垫后，对你的文件加密之后再进行勒索。

比特币病毒从何而来

加密算法勒索病毒其实是个“老朋友”了，世界上第一个有记录的勒索软件Cryptolocker诞生于1989年，它其实就是一种用加密算法来勒索钱财的程序，后来，病毒制造者没几天就被抓获了。

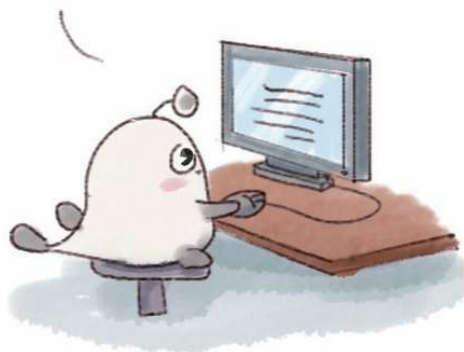


图2 - 27Cryptolocker病毒制造者被抓获

其实，Cryptolocker最开始是很好破解的，因为它最开始使用的是对称加密算法，编个程序逆向破解一下就可以了，但是，现在流行的勒索病毒Wallet、Onion使用的却是非对称加密算法。非对称加密算法的加密和解密过程使用两个密钥，因此，单纯靠逆推是不可行的，我们在后面会具体讲解一下。

然而，这次的黑客不仅改进了勒索蠕虫病毒，还搭配了一个“好伙伴”——“永恒之蓝”黑客工具，不需要你点击任何链接，它就可以直接占领你的计算机。“永恒之蓝”病毒还有一个美丽的传说，据说它原本是美国国家安全局用来窃取其他国家信息的工具，是“美国武器库”中的一种。美国国家安全局旗下有一个黑客组织叫“方程式组织”，负责替美国政府做一些不可告人的事情，后来，因为闻名天下的伊朗核试验的“震网”事件以及后来的“棱镜门”事件逐渐为人所知。

我使用对称加密算法,可以逆向破解



以前

我使用非对称加密算法,不能逆推



现在

图2-28非对称加密算法无法逆推



图2-29“美国武器库”的传说

后来,有个叫“影子经纪人”的黑客团队,把“美国武器库”破解了。然后,他们在网上拍卖,想把这些“武器”换成钱。然而,没人理他们,

于是，他们发起众筹，企图利用这些“武器”赢利，依然没什么人理他们。最后，一气之下，在2017年4月14日，他们直接把这批“武器”公开了。于是“永恒之蓝”黑客工具和加密算法勒索病毒就成为一款“杀伤性武器”。



图2-30 影子经纪人的传说

当然，这件事只是一个美丽的传说，美国国家安全局也没有承认，所以，“永恒之蓝”究竟从何而来众说纷纭，并没有实际考据。

这个病毒什么时候能破解

首先，“永恒之蓝”黑客工具是利用Windows（微软公司的操作系统）漏洞来攻击的，也就是说，只要更新Windows补丁，并开启防火墙的主动防御，基本上，这个工具就没有了生存的土壤，然而，Windows漏洞总是不断更新，说不定什么时候黑客搭配一个攻克新款漏洞的工具，就又生出了各种变种病毒，比如“永恒之红橙黄绿青蓝紫”之类的。

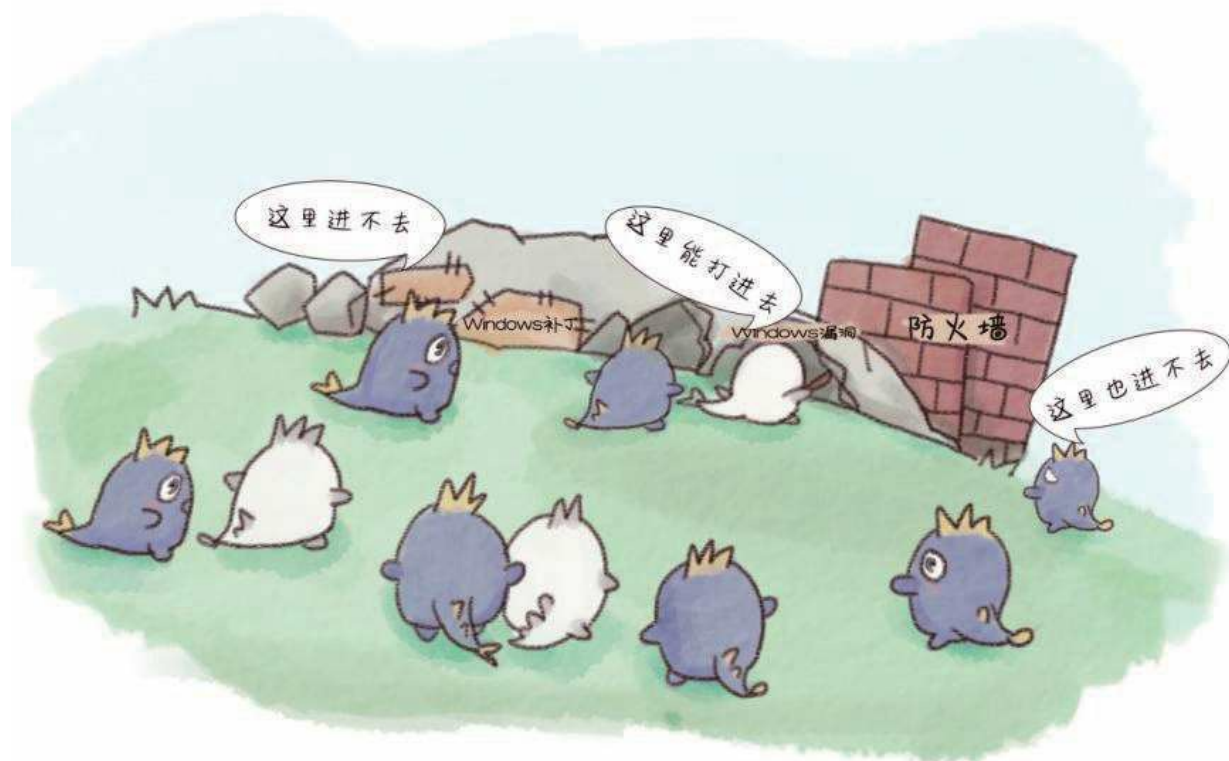


图2-31 升级防火墙

我们知道，勒索病毒使用非对称加密算法进行加密，其最突出的特点就是不可篡改和不可逆，加密和解密过程使用的是两个不同的密钥。



图2 - 32非对称加密算法不好破解

现在的计算机无法完成倒推所需要的计算量，或者说，算出来的成本太高了。现在全球热议的最领先的区块链技术使用的就是非对称加密算法，也就是说，黑客是站在时代最前沿的科技的肩膀上设计密码，我们想要破解没那么容易。



图2-33 站在巨人的肩膀上

我们可以回想一下那个家喻户晓的“熊猫烧香”病毒最后是怎么被破解的？写病毒的黑客被抓住之后，自己编了套程序破解了，而这次的情况也类似，最可能的解决方法就是，把黑客抓住之后，让黑客把他手里的密钥交出来，我们输入密钥之后就可以解封了。



图2-34 黑客交出密钥

为什么只要比特币

黑客到底什么时候会被抓到，怎么抓？这就涉及我们探讨的第三个问题了，为什么黑客非要用比特币支付呢？因为比特币的匿名性，换句话说，你不容易抓住他。比特币是一种网络虚拟货币，可以在全世界流通，具有匿名性，这便于黑客隐藏身份。你不需要知道对方是谁，只需要一个比特币地址就可以点对点地给对方打款。同时，比特币的世界性和流动性也是黑客选择比特币的理由，比特币在数字货币中占有最大的份额，它在全世界中拥有很多“粉丝”，很多国家都承认了比特币的合法地位，一些大型企业也接受比特币支付。



图2-35 比特币的全球性

但是，黑客想要逃脱法网也不是那么容易的，因为比特币的特点之一就是不可篡改，所有的记录都是无法篡改的，并且公开可查。一旦黑客公布的比特币地址收到了比特币，那么账本上就多了一笔记录，每个人手里的账本会同步更新。每个人都能查到这个记录，之后这个地址的

各种转账、提现记录也都是可查的。只要黑客进行了比特币提现这类需要和现实交互的操作，就一定会露出蛛丝马迹。



图2-36比特币交易记录公开可查

实际上，在大多数情况下比特币本身并不是百分之百匿名的。发送和接收比特币，就像作者用笔名发表作品一样。如果一个作者的化名和他的身份联系在一起，他曾经写下的任何东西都会与其联系在一起。

对于个体来说，比特币的匿名性与你接收比特币的钱包有关。涉及该地址的每一项交易都将永久保存在该区块链中。如果你的地址和你的真实身份相关，那么每一项交易都会和你有关。

现在，许多国家都把比特币交易平台纳入监管范围，交易需要多重实名认证。因此，只要黑客露出与现实相关的蛛丝马迹，就有可能被抓到。

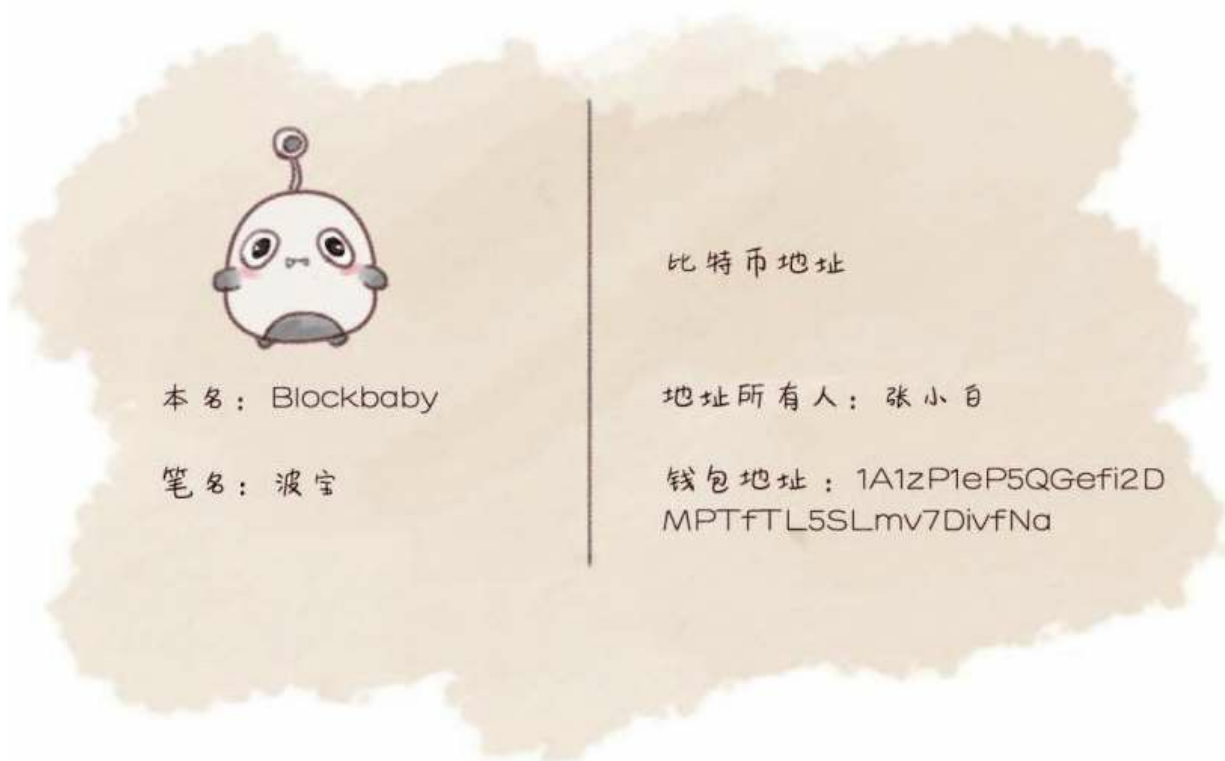


图2-37比特币并不是百分之百匿名

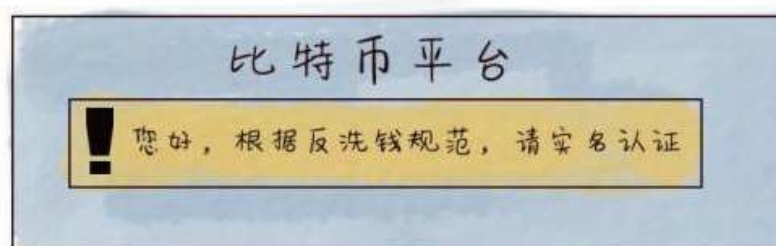


图2 - 38多重实名认证

怎么预防“永恒之蓝”病毒

第一招：搜索

现在，请打开你的任何一个浏览器，在输入框里输入“如何预防比特币病毒”，你就会发现铺天盖地的解决方法，随便找一个点开看就行了，毕竟都一样，无非是断网、设防火墙、阻止445端口、升级Windows补丁。在这里，建议大家都养成长期打开防火墙的习惯，虽然Windows的防火墙总是时不时弹出，但是，安全终归最重要。

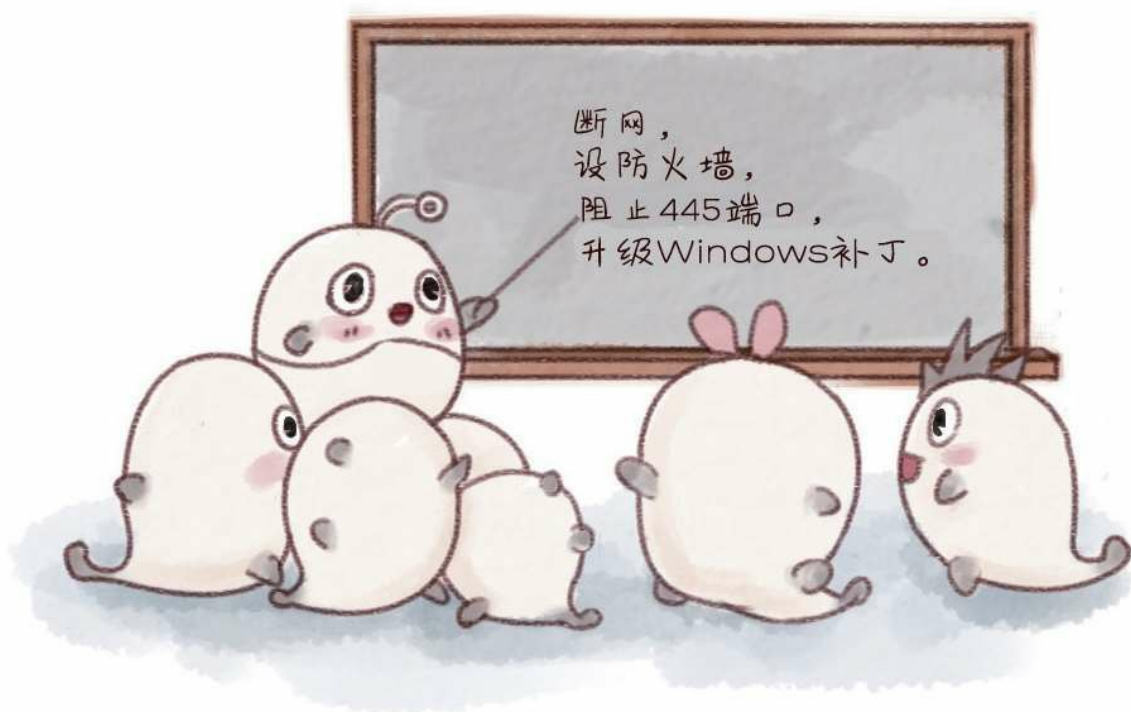


图2 - 39第一招：搜索

第二招：以毒攻毒

预防了这次的病毒攻击，下次再遇到怎么办呢？你可以尝试这么操作：黑客不是要加密我们的重要文件吗，比如后缀为doc（文档）、xls（电子表格）、ppt（演示文稿）、psd（图片文件）之类的文件；而对于一些冷门格式的视频和种子文件，黑客总不会加密吧，所以，除了重要文件要多备份几遍之外，我们还可以把所有的重要文件做成压缩包，然后改成一个莫名其妙的格式（比如后缀为“modv”）。当然，这一招并不能完全断绝重要文件被破坏的可能性。

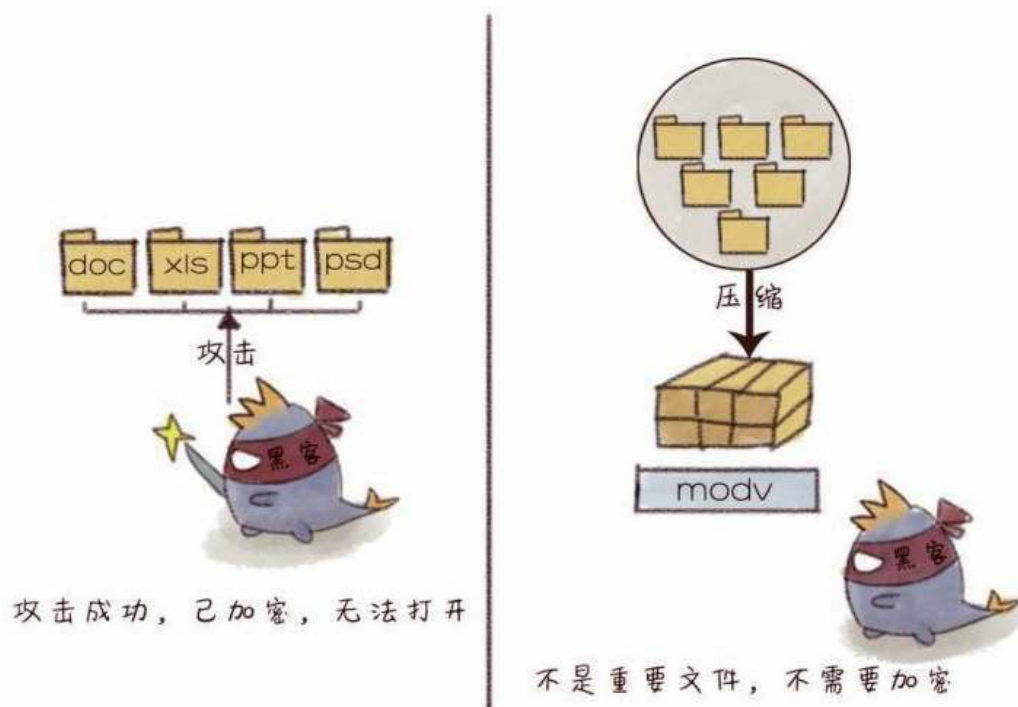


图2-40第二招：以毒攻毒

第三招：占坑抢位

这一招最绝的一点就在于，走黑客的路，让黑客无路可走，所以适用于程序员：自己编一套经非对称加密的“病毒程序”，把自家电脑的文件都加密，密钥保存在自己手里，每次查看前先输一遍密钥。这样就是麻烦点，但是它有用啊！“此坑是我的，想毒我，没门儿！”



图2-41 第三招：占坑抢位

最后需要说的一点是，目前中国的比特币平台是不能提现的，因此，若想要缴纳赎金也需要谨慎考虑。毕竟，我们并不知道缴纳赎金之后是否能百分之百地解锁并免受病毒的二次入侵。面对病毒，我们需要冷静，再冷静啊。



图2-42 缴纳赎金后解锁失败

其实，作为和区块链、比特币相关的从业者，从病毒暴发的那一刻开始，我就收到七大姑八大姨的各种电话问候：听说你们公司研究的玩意儿都成病毒了，你们公司不会跑路吧……白天被各种围追堵截询问：您好，请发表一下对此事的看法，到底什么时候才能抓到？

比特币之所以被黑客当作勒索的工具，确实是因为它具有匿名性、去中心化等方便黑客隐藏身份的某些特性，但我始终认为，技术本身是无罪的，比特币抑或区块链都不应该背黑锅。



图2-43技术本无罪

比特币的工作流程

如图2-44所示，在区块链中，所有的节点向上回溯，都会到达源头，即区块链中的第一个区块，也就是“创世区块”。

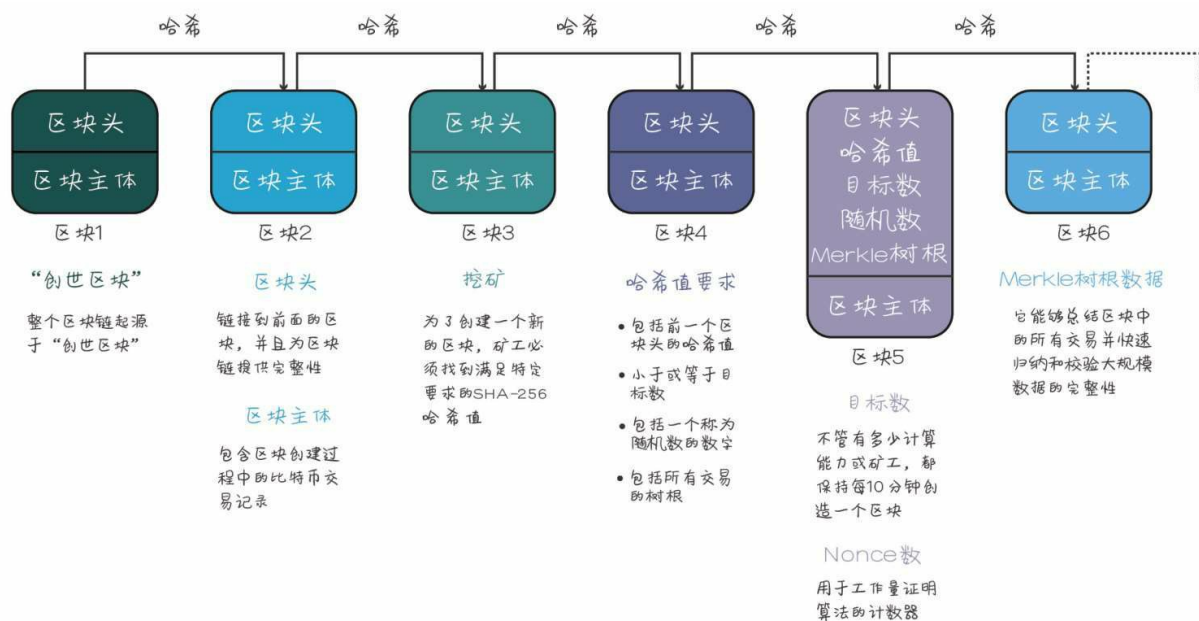


图2 - 44比特币工作流程

在“创世区块”诞生之后，比特币的用户通过不断地“做题”，即通过计算寻找满足特定SHA-256哈希值对应的数值解。这个过程就是比特币中的“挖矿”。[\[7\]](#)

当任意一个用户优先计算出符合要求的数值解时，就会在全网范围内广播，而网络中的其他节点收到这条信息会进行验证，若通过验证，其他节点就会放弃计算，并将新创建的区块加到前一个区块的后面。

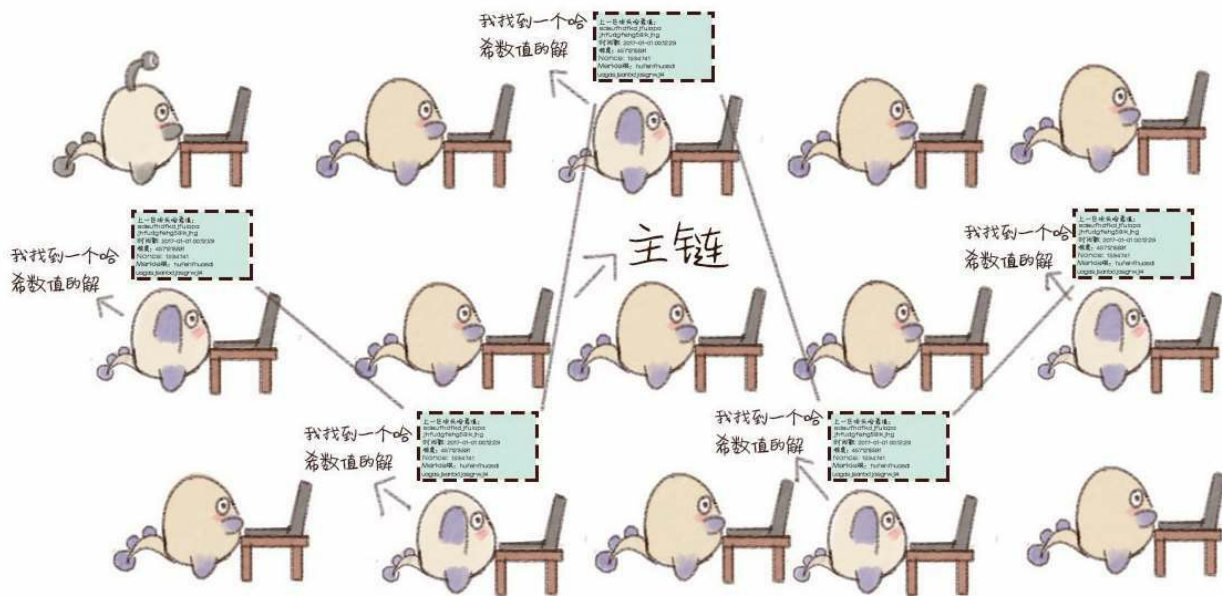


图2 - 45 计算特定哈希值的数值解

随着越来越多的人加入比特币的区块链系统，一个又一个哈希值的数值解被找到，在不断重复的过程中，新的区块不断地生成、验证，最终形成一个主链。同时，哈希算法的难度也会调整，以此控制用户们解出数据所用的时间。

而在比特币的实际交易过程中，假设比特币中的用户A和B之间要完成一个交易，包含这笔交易的区块向区块链中的所有用户发布广播，全网用户通过验证哈希值来确认这笔交易是否有效，一旦被认证为有效，这个区块就会被加盖时间戳，然后被添加到区块链主链上。

向全网用户广播

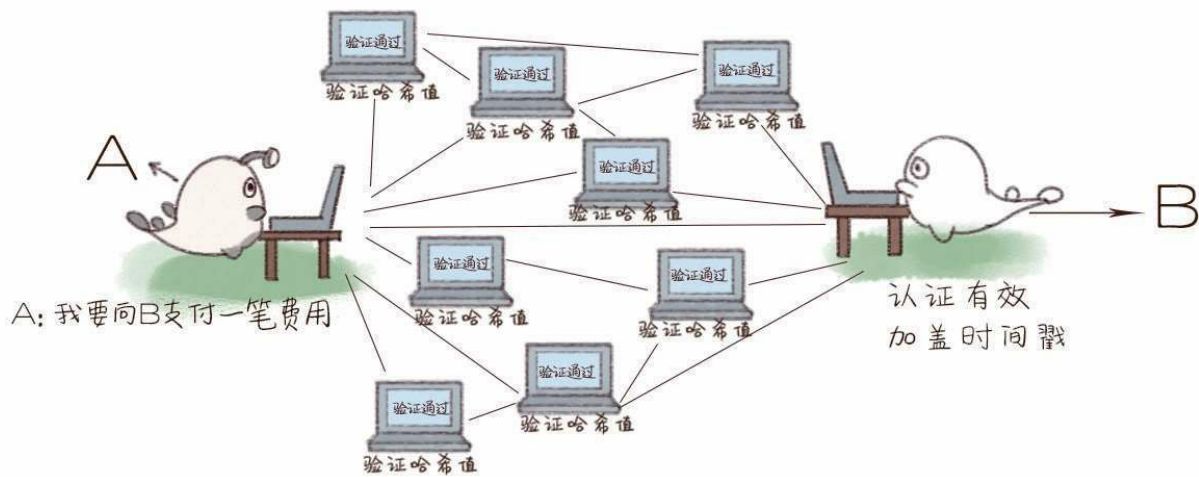


图2-46 加盖时间戳

区块链的本质是一个互相验证的公开记账系统。这个系统所做的事情，就是记录所有账户发生的所有交易。每个账号的每笔数额变化都会被记录在全网总账本中。而且每个人手上都有一份完整的账本，每个人都可以独立统计出有史以来比特币系统每个账号的所有账目，也能算出任意账号当前余额是多少。[\[8\]](#)

由于所有数据公开透明，任何人都可以去查看它的源代码，人们便会信任这套去中心化的系统，而不担心里面是否隐藏着什么阴谋。

比特币会硬分叉吗

2009年比特币诞生，如今，其市值已达数百亿美元，众多人为之疯狂（注意，根据政策规定，比特币不是货币）。最近，有人预测，比特币到了不得不分叉的时候，甚至可能会暴跌。

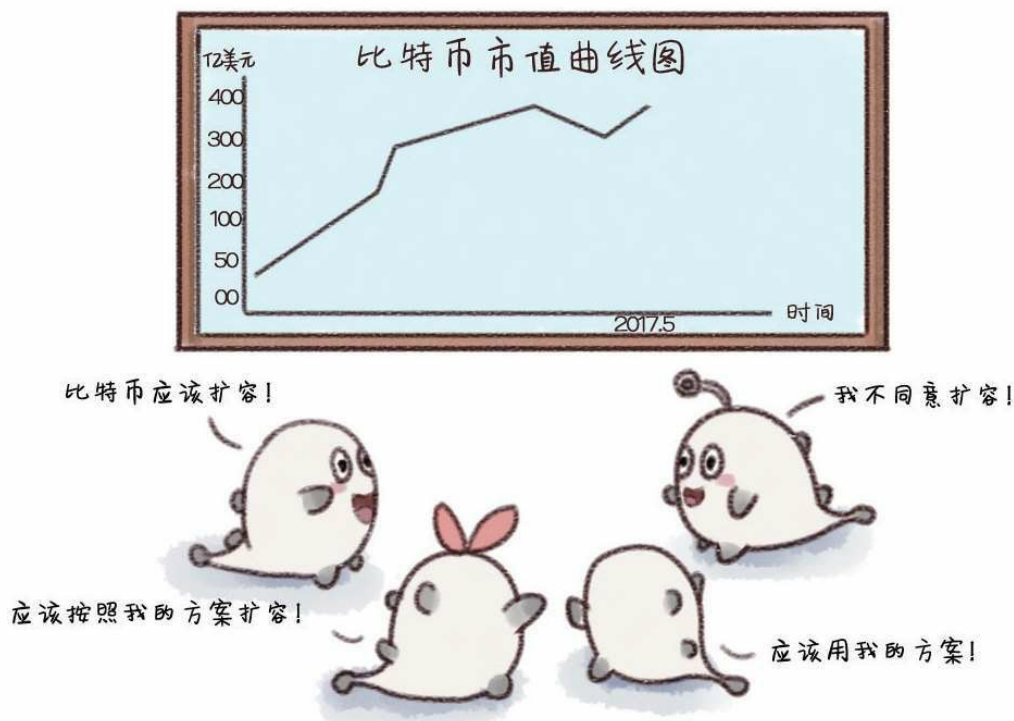


图2-47 比特币会分叉吗

一、中本聪拍了下脑袋

中本聪在设计比特币的时候，是2009年，那个时候数据能有多少？更何况也没有多少人使用比特币。于是他一拍脑袋决定了，比特币中一个区块的容量就是1M（兆字节）吧。而一笔交易是250字节甚至更多，现在一些交易基本达到了500字节。容量不够用啊！

我们来算笔账：

比特币一个区块的容量是1M，

$1\text{M}=1\,024\text{KB}$ （千字节） $=1\,048\,576$ 字节，

那么一个区块包含的交易总数为： $1\,048\,576 \div 250 \approx 4\,194.3$ （笔）。

比特币中一个区块确认的时间是10分钟，

10分钟=600秒，

那么一个区块每秒能处理的交易数为： $4\,194.3 \div 600 \approx 7$ （个）。



图2-48 1M的容量不够用

如果一个区块每秒只能处理7笔交易，要是交易数据再大点，可能连7笔都达不到。这样会造成一个结果，比特币上的交易拥堵而缓慢。一笔交易发生之后，前面还有好多交易在排队等待确认，到底要等到什么时候啊？总有一天堵塞到一定程度就会超过容量极限，然后就崩溃了！

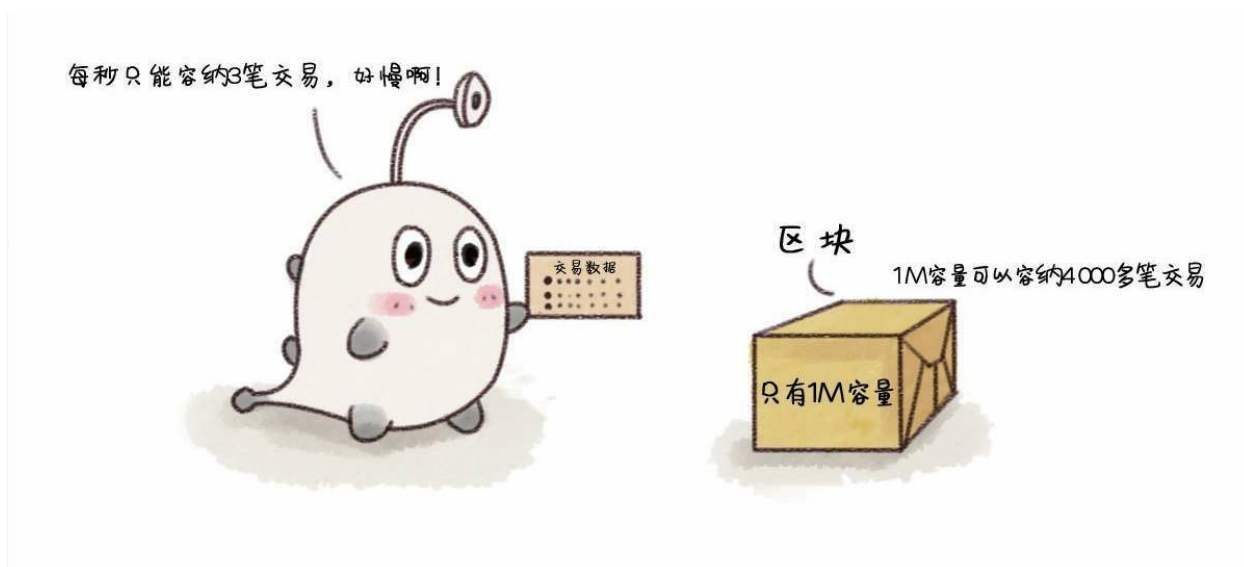


图2-49 区块需要扩容

二、扩容方案意见不一

出了问题怎么办呢？改啊！

怎么改啊？中本聪消失了啊！

那找谁啊？中本聪把系统维护交给了5个极客！

哦，怎么改啊？

听我的，改成2M；不，听我的，改成20M！

很多人代表各方的利益群体提出了自己的扩容方案！

1. Bitcoin Classic（比特币经典版），此方案认为应该将这个字段的最大值调到2M，并且以后有计划取前2 016个区块大小的中位数再乘一个约定好的倍数来决定下一批区块的大小上限。

2. Bitcoin XT（比特币新版），此方案认为这个值应该修改为20M，并且每两年翻一番，直到上限值达到8.3G（千兆字节）。

3. Bitcoin Unlimited（比特币无限版），此方案认为这个值多大都行，甚至可以无限大，由矿池决定其大小。



图2-50 扩容方案意见不一

每个人都觉得自己是对的，谁也说服不了谁，怎么办啊？比特币不升级了？不行啊，还是要升级的！那么问题就来了，要是做出一个升级版本，所有人都直接升级成了新版，就没有分叉问题了，全世界大升级大和谐啊。但是，有人的地方就有纷争，有的人升级，有的人不升级。这可好了，乱套了，用的系统都不一样，那要如何统一呢？

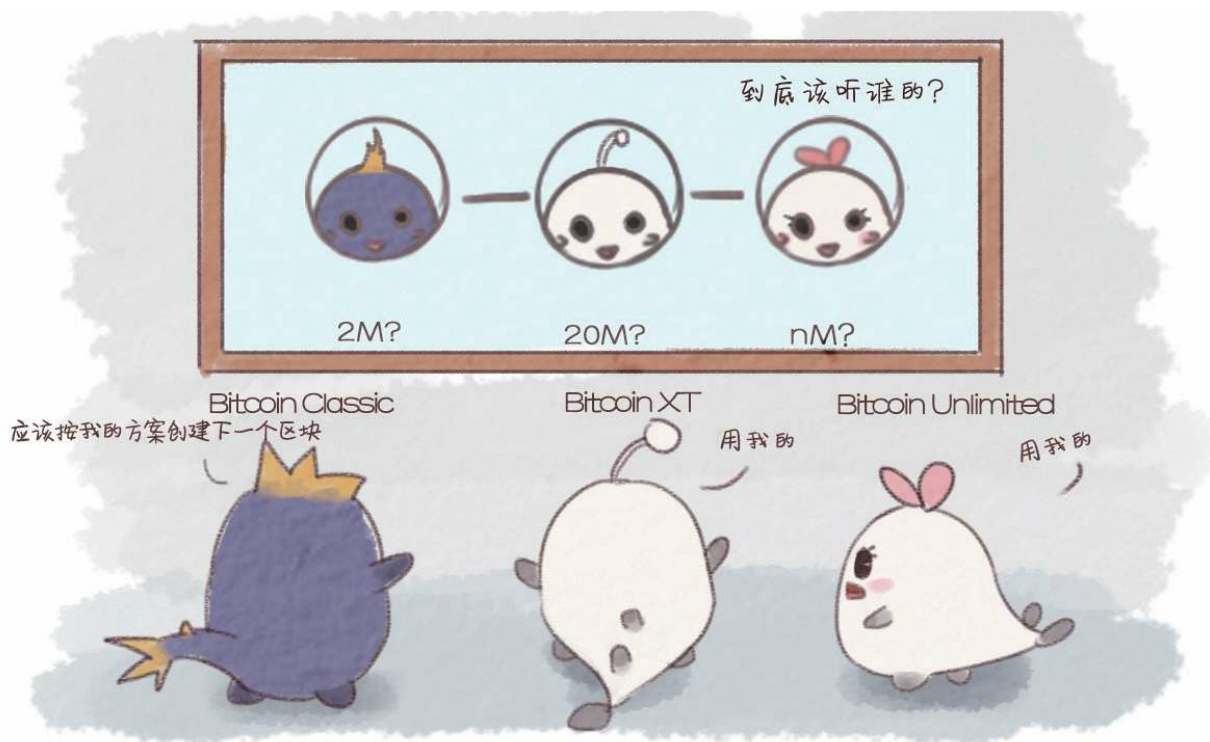


图2-51 方案不同可能会导致分叉

不同的理念催生出了多种扩容方案，各个方案间无法统一，于是比特币分叉了。其实，随着时间的流逝，方案所提出的容量大小也随之增长，莫非，这不是价值观的原因而是世界观的原因？

三、硬分叉和软分叉

分叉怎么还分软硬呢？简单来说就是兼容性的不同，软分叉是暂时的，硬分叉是永久的。

区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。



图2 - 52 硬分叉结构图

硬分叉的定义是这样的：硬分叉是指比特币的区块格式或交易格式（这就是广泛流传的“共识”）发生改变时，未升级的节点拒绝验证已经升级的节点生产出的区块，不过已经升级的节点可以验证未升级节点生产出的区块，然后大家各自延续自己认为正确的链，所以分成两条链。[\[9\]](#)



图2-53 硬分叉是什么

硬分叉的特点如下：

1. 没有向前兼容性，之前的版本将不可再用，需要强制升级；
2. 在区块链层面会有分叉的两条链，一条旧链，一条分叉新链；
3. 需要在某个时间点全部同意分叉升级，不同意的将会进入旧链。[\[10\]](#)

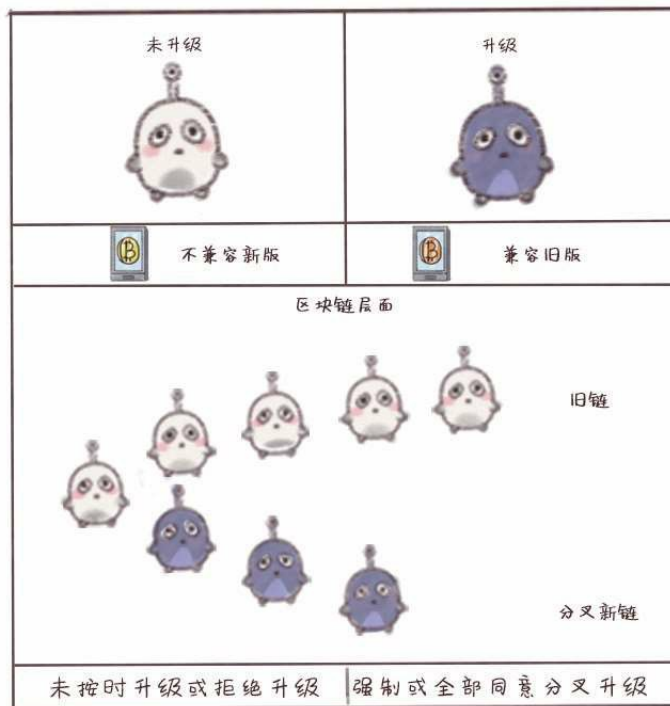


图2 - 54硬分叉的特点

当新共识规则发布后，没有升级的节点由于不了解新共识规则，就会生产不合法的区块，从而产生临时性分叉。

软分叉的定义是这样的：

软分叉是指比特币交易的数据结构发生改变时，未升级的节点可以验证已经升级的节点生产出的区块，而且已经升级的节点也可以验证未升级的节点生产出的区块。[\[11\]](#)

软分叉



图 2-55 软分叉结构图



图2-56 软分叉是什么

软分叉的特点如下：

1. 有较好的兼容性，之前版本的部分功能可用，可不升级；
2. 在区块链层面没有分叉的链，只是组成链的区块有新区块和旧区块之分；

3. 相当长的时间里，可允许不进行升级，继续使用原版本生成旧区块，与新区块并存。



图2-57 软分叉的特点

四、举几个有趣的例子

我们模拟一种极端的情况，抽象出一个比特币王国来解释所谓的新系统的兼容性问题。在遥远的岛上，有一个比特币王国，大家相安无事地生活了很多年，由于王国设施陈旧，存在着这样那样的问题，于是大家开始讨论解决方案。

有人觉得应该推翻了重新修葺，并且上书了一本“如何建造一个华丽的王国”的奏书，里面有九九八十一种推翻重建的方案。有些人认为补补窟窿，刷刷墙还是勉强可以看，根本不用大动干戈。两派争论不

休，无法达成一致，这就引起了分叉。

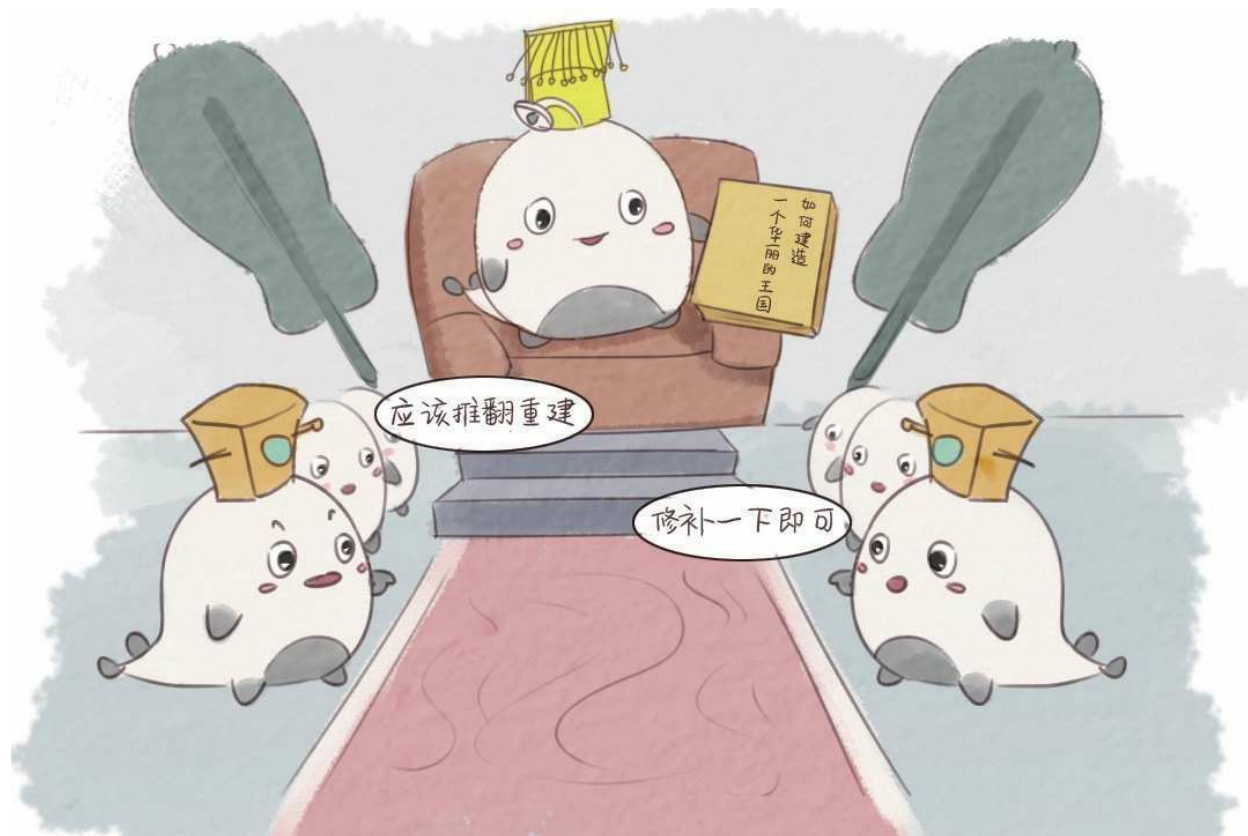


图2-58 比特币王国的例子

什么情况下会出现硬分叉呢？派系争论不休，于是开始各干各的。提议推翻重建的人雇了几十个民工，新的建筑焕然一新，王国里新旧建筑的风格相当不统一。这就相当于比特币世界里的硬分叉，表现在比特币世界里就是从新的节点开始，分成了两条链——旧链和新链，两条链互不兼容。



图2-59 打个比方说明硬分叉

软分叉会出现什么结果呢？派系争论不休，但要求重建的一派有了妥协的意愿，同意让装修装饰派试一试他们的方案。于是装修队开始对墙上的破洞进行修补，把陈旧的颜色换成鲜艳的颜色。这时，王国里正常的生活仍然在继续。新旧面貌共存。表现在比特币上就是未升级的节点按照以前的规则继续计算，但已经升级的节点仍然按照扩容后的规则计算。因此，Bitcoin Core（比特币核心钱包）主张的Segwit（隔离见证）升级后，比特币依旧是比特币，不会有新的币种诞生。



图2-60 打个比方说明软分叉

五、分叉有什么影响吗

说到影响，我们看看近来比较成功的一次分叉。

2016年7月，以太坊开发团队通过修改以太坊软件的代码，在第192000区块，强行把The DAO（分布式自治组织）及其子DAO的所有资金全部转到一个特定的退款合约地址从而“夺回”黑客所控制的DAO合约的以太币。

之后，便形成两条链，一条为ETC（原链），一条为新的ETH（分叉链），以太坊成功地硬分叉了！

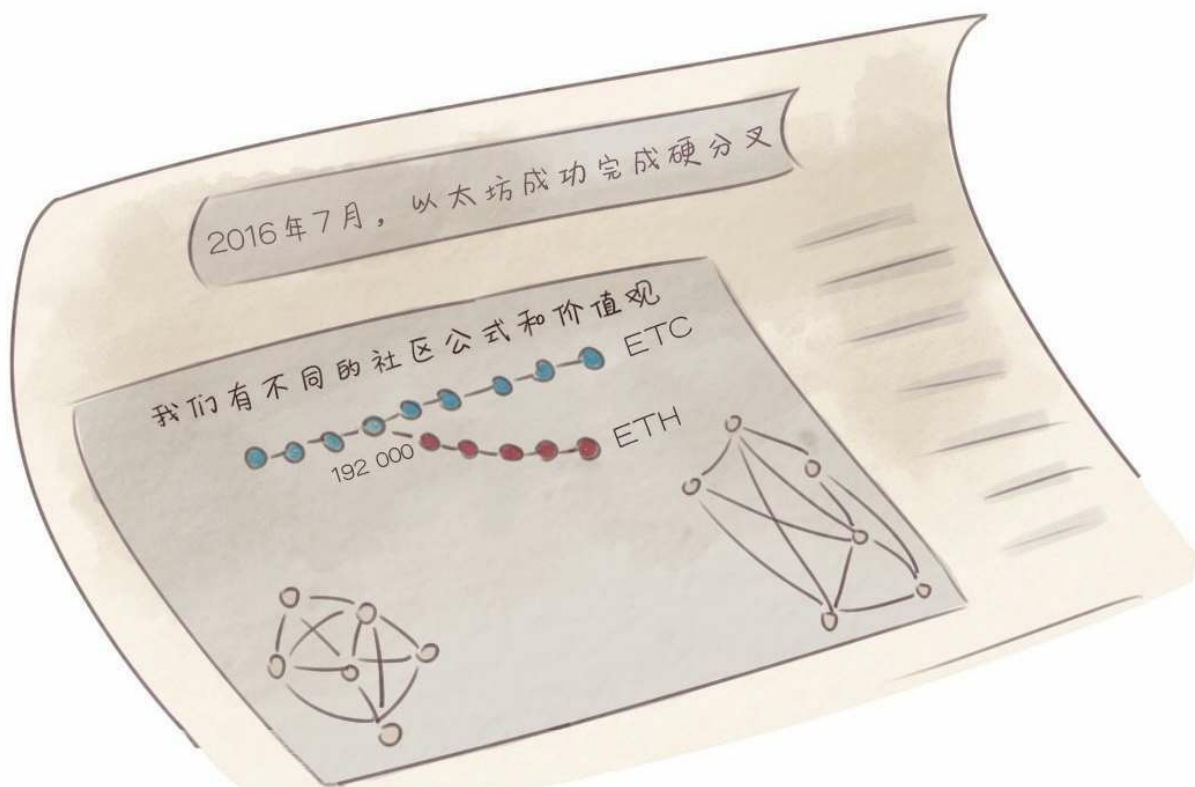


图2-61 以太坊的硬分叉

硬分叉对比特币矿工的影响：

硬分叉这事能闹起来，矿工绝对出了大力气。一旦分叉，矿工挖矿便简单了，可以挖到更多币了，多开心啊，但是，他挖出来的币值不值钱还得看有没有人买，毕竟市场决定价格。

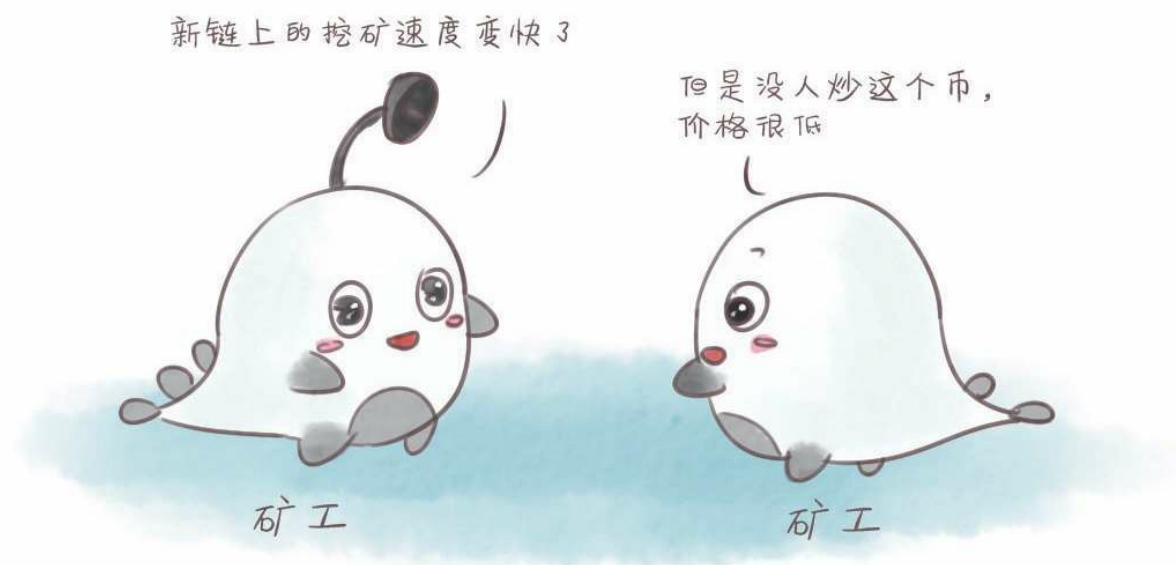


图2-62 对矿工的影响

硬分叉对比特币产业链的影响：

从技术角度来看，硬分叉的主要问题是它需要所有用户转移到具有不同规则的新区块链。为了保持比特币的品牌价值和对比特币的信仰，比特币的支持者是反对硬分叉的。如果真的硬分叉，将会掀起一场彻底的网络战和舆论战。

硬分叉对币价的影响：

再说一句，分叉后比特币的币价是涨还是跌，前景究竟会如何发展，由市场的选择决定。按常理来看，估计分叉后比特币会先暴跌一场，然后分叉后的两个币种经过时间的洗礼后会渐渐回归理性，毕竟分叉后的“1+1”肯定不等于2。

快加入新链，
我们制定了新的规则

我们觉得旧链很好，
拒绝加入



新链用户



旧链用户

图2-63 对产业链的影响

比特币的币价走势



图2-64 硬分叉对币价的影响

比特币分叉仿佛是一个一旦开始就永不会落幕的会议，但这也正是去中心化的比特币的魅力之所在。

区块链的工作原理

那么，区块链究竟是如何工作的呢，如图2-65所示，我们假设A和B之间要发起一笔交易，A先发起一个请求——我要创建一个新的区块，这个区块就会被广播给网络里的所有用户，所有用户验证同意后该区块就被添加到主链上。这条链上拥有永久和透明可查的交易记录。全球一本账，每个人都可以查找。

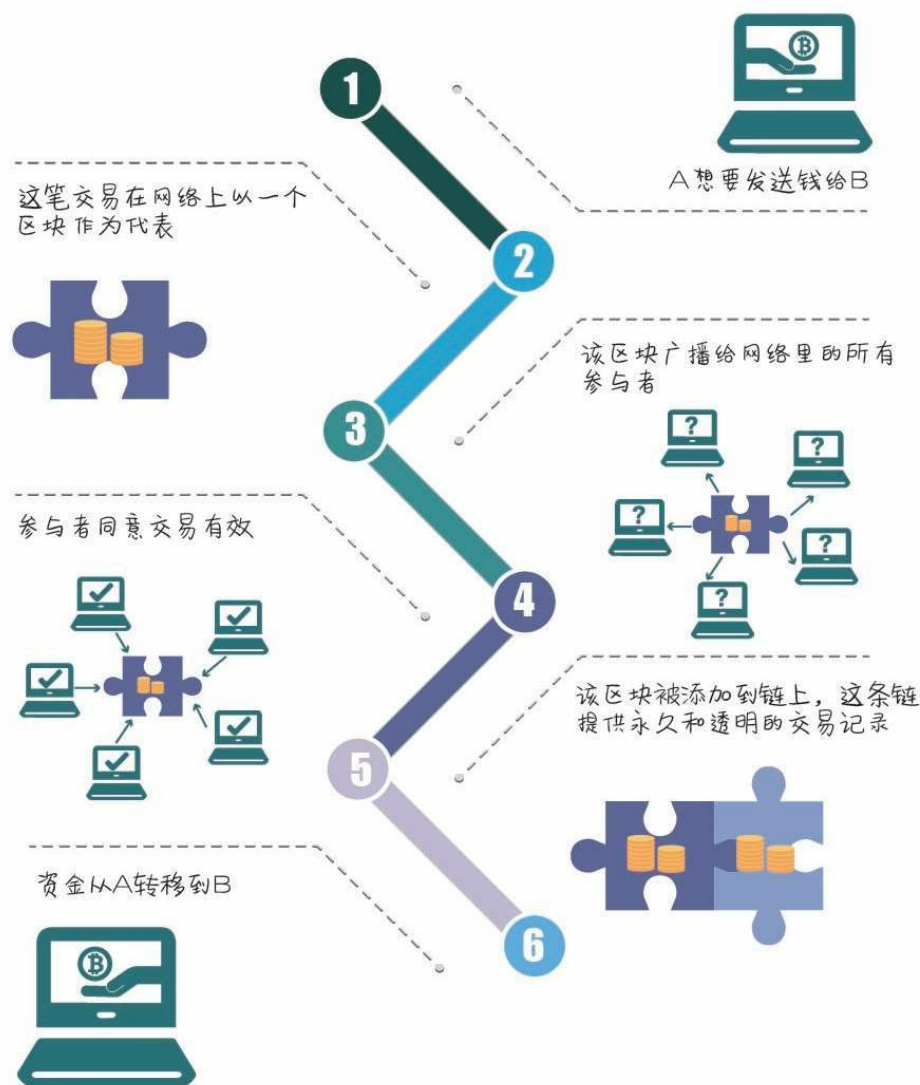


图2 - 65 区块链的工作原理

区块链技术实际上是一个分布式数据库，在这个数据库中记账不是由个人或者某个中心化的主体来控制的，而是由所有节点共同维护、共同记账的。所有的单一节点都无法篡改它。

如果你想篡改一个记录，你需要同时控制整个网络超过51%的节点或计算能力才可以，而区块链中的节点无限多且无时无刻都在增加新的节点，这基本上是不可能完成的事情，而且篡改的成本非常高，几乎任何人都承担不起。

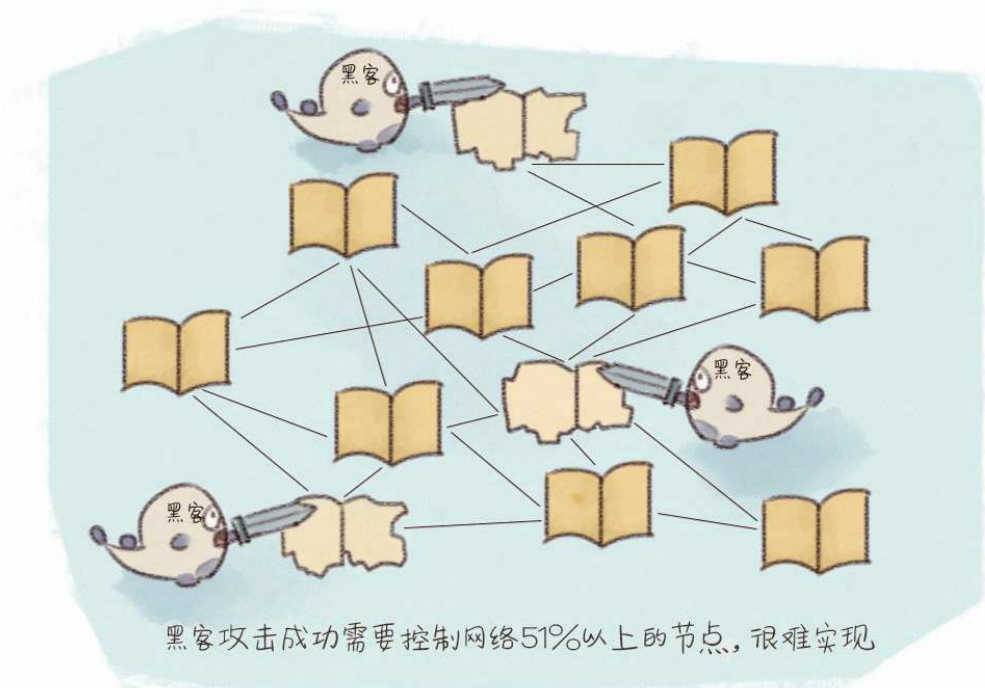


图2-66 篡改账本无法实现

区块链的四大特点

经过无数次的记账，区块链就成为一个可信赖、超容量的公共账本。它具有以下几个特征：[\[12\]](#)

1. 去中心化：在一个去中心化的金融系统中，没有中介机构，所有节点的权利和义务都相等，任意节点停止工作都不会影响系统整体的运作。

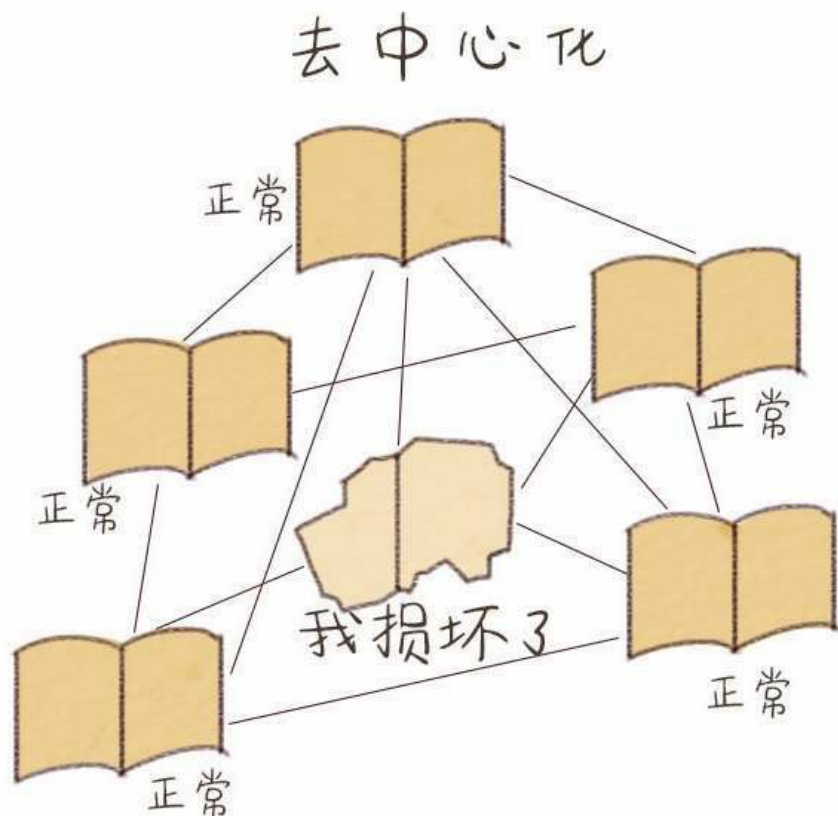


图2-67 区块链特点之去中心化

2. 去信任：系统中所有节点之间无须信任也可以进行交易，因为数据库和整个系统的运作是公开透明的，在系统的规则和时间范围内，节点之间无法欺骗彼此。

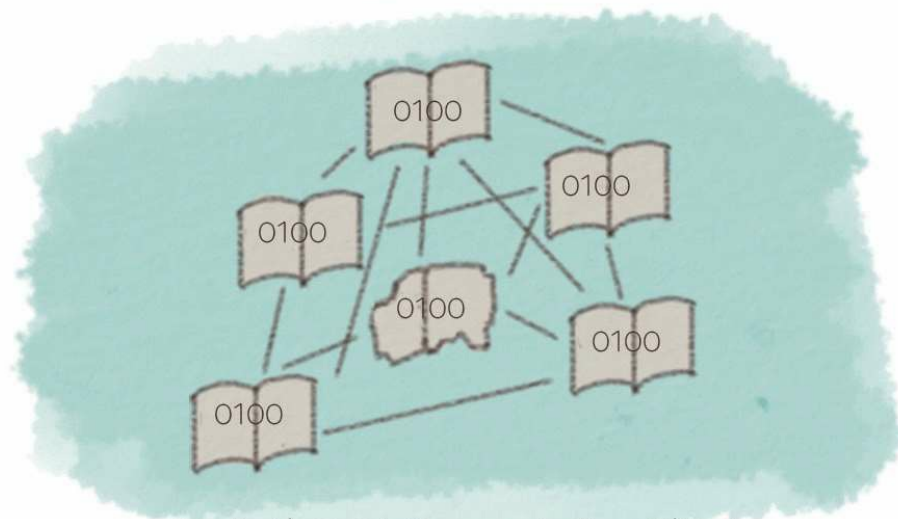
去信任



图2 - 68 区块链特点之去信任

3. 集体维护：系统是由其中具有维护功能的所有节点共同维护的，系统中所有人共同参与维护工作。

集体维护



我们共同维护，一个都不能少

图2 - 69 区块链特点之集体维护

4. 可靠的数据库：系统中每一个节点都拥有最新的完整数据库拷贝，修改单个节点的数据库是无效的，因为系统会自动比较，认为最多次出现的相同数据记录为真。

可靠的数据库

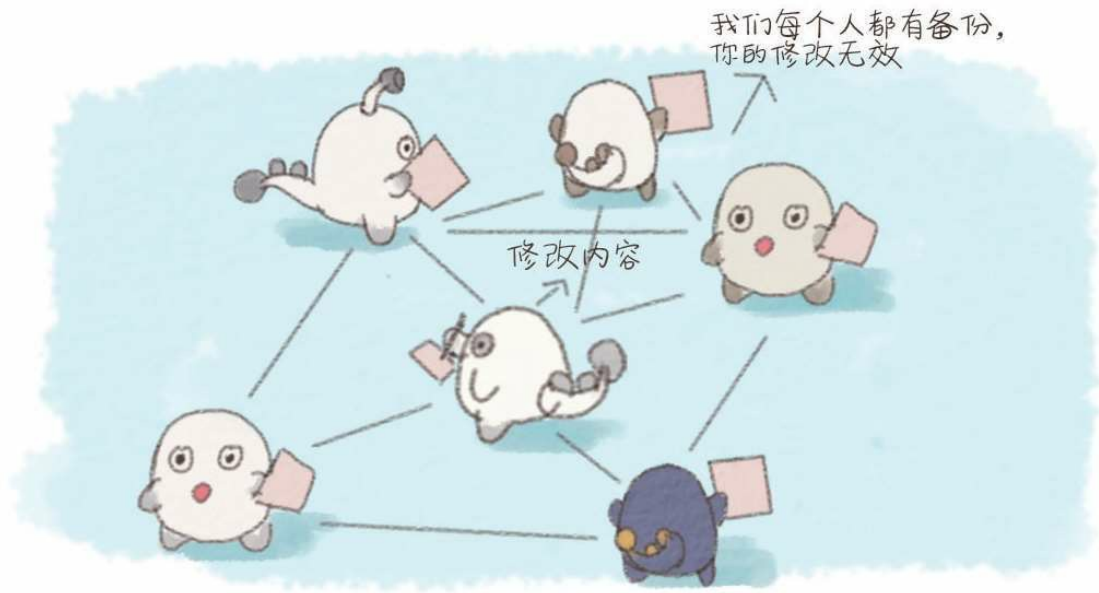


图2-70 区块链特点之可靠的数据库

讲几个问题，区块链底层架构

区块链的模型架构

有关区块链的模型结构问题，已经被谈论千遍万遍了，基本已经成为一种定义式的问题了，我们将使用诸多资料中相对较为全面，也较容易理解的一类解释来向大家阐述。

区块链基础架构分为6层，包括数据层、网络层、共识层、激励层、合约层、应用层。每层分别完成一项核心功能，各层之间互相配合，实现一个去中心化的信任机制。

一、数据层

数据层主要描述区块链技术的物理形式。区块链系统设计的技术人员们首先建立的一个起始节点是“创世区块”，之后在同样规则下创建的规格相同的区块通过一个链式的结构依次相连组成一条主链条。随着运行时间越来越长，新的区块通过验证后不断被添加到主链上，主链也会不断地延长。

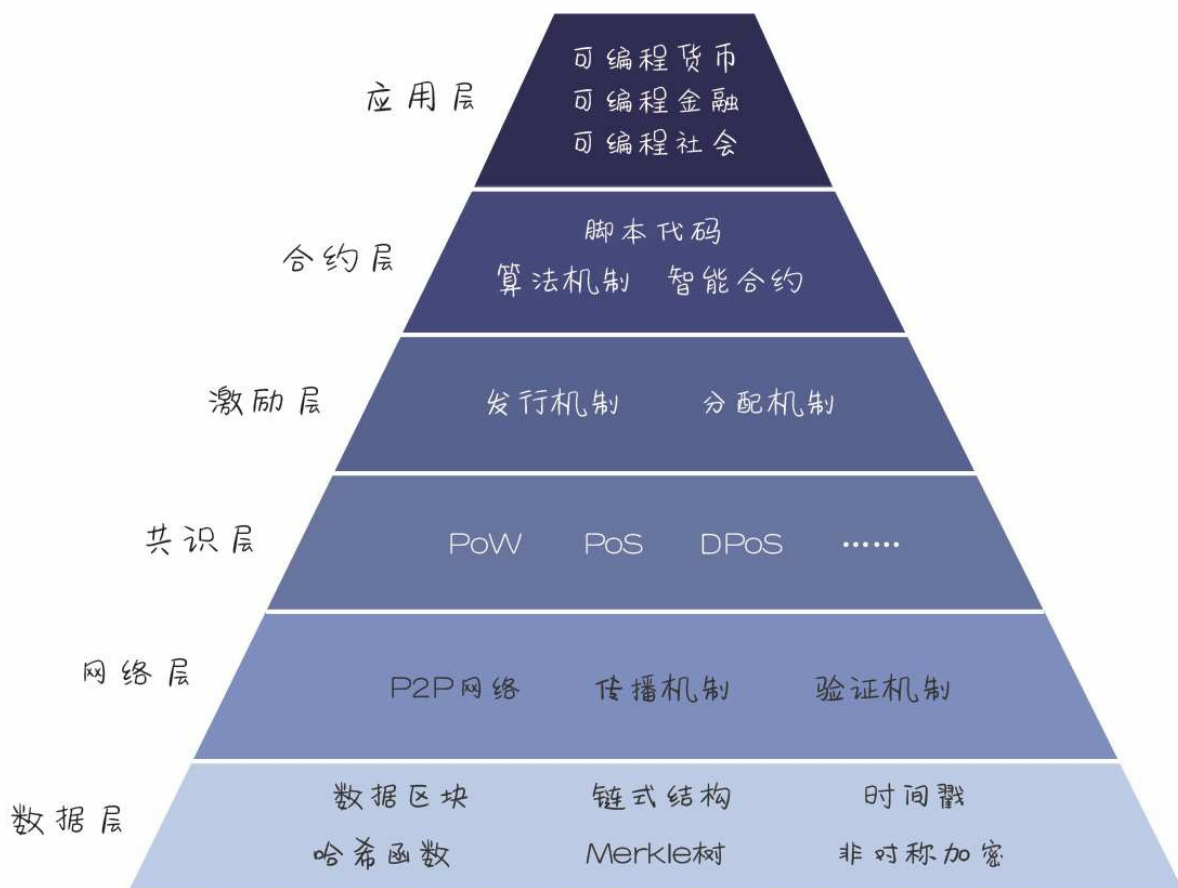


图2 - 71 区块链的模型架构

每个区块中也包含了许多技术，比如时间戳技术，它可以确保每一个区块按时间顺序相连接；再比如哈希函数，它能够确保交易信息不被篡改。

二、网络层

网络层的主要目的是实现区块链网络中节点之间的信息交流。区块链网络本质上是一个P2P（点对点）网络。每一个节点既接收信息，也产生信息。节点之间通过维护一个共同的区块链来保持通信。[\[13\]](#)

区块链的网络中，每一个节点都可以创造新的区块，在新区块被创造后会以广播的形式通知其他节点，其他节点会对这个区块进行验证，

当全区块链网络中超过51%的用户验证通过后，这个新区块就可以被添加到主链上了。

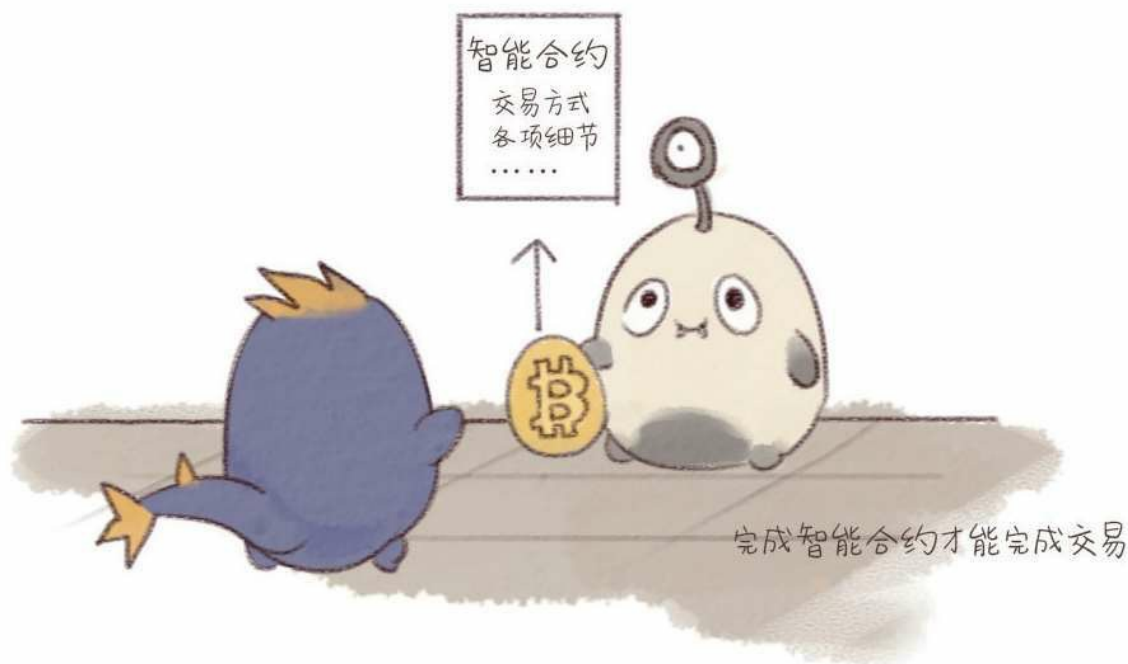


图2-72 区块链的网络层

三、共识层

共识层能让高度分散的节点在去中心化的系统中高效地针对区块数据的有效性达成共识。区块链中比较常用的共识机制主要有工作量证明、权益证明和股份授权证明三种，我们在下面的章节中会重点讲解。

四、激励层

激励层的主要功能是提供一定的激励措施，鼓励节点参与区块链的安全验证工作。我们以比特币为例，它的奖励机制有两种。在比特币总量达到2 100万枚之前，奖励机制有两种，新区块产生后系统奖励的比特币和每笔交易扣除的比特币（手续费）。而当比特币总量达到2 100

万时，新产生的区块将不再生成比特币，这时奖励机制主要是每笔交易扣除的手续费。



图2-73 区块链的激励层

五、合约层

合约层主要是指各种脚本代码、算法机制以及智能合约等。我们以比特币为例，比特币是一种可编程的货币，合约层封装的脚本中规定了比特币的交易方式和过程中涉及的种种细节。

六、应用层

应用层封装了区块链的各种应用场景和案例，比如基于区块链的跨境支付平台OKLink，以及在“应用篇”中我们将讲到的五花八门的应用。

区块链的基本类型

一、公有链

公有链是指全世界任何人都可读取、任何人都能发送交易且交易能获得有效确认，任何人都能参与共识过程的区块链——共识过程决定哪个区块可被添加到区块链中，同时明确当前状态。[\[14\]](#)

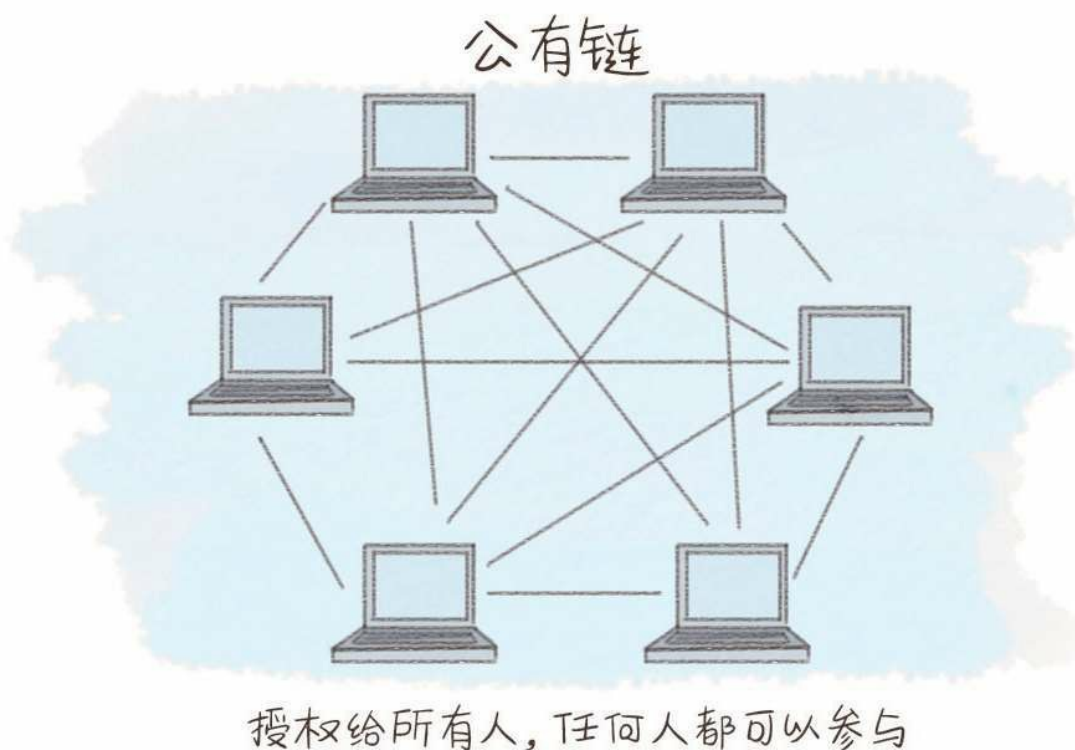


图2-74区块链的公有链

公有链有如下几个特点：

1. 保护用户免受开发者的影响

在公有链中程序开发者无权干涉用户，区块链可以保护其用户。

2. 访问门槛低

任何人都可以访问，只要有一台能够联网的计算机就能够满足基本的访问条件。

3. 所有数据默认公开

公有链中的每个参与者可以看到整个分布式账本中的所有交易记录。

二、私有链

私有链是指其写入权限仅在一个组织手里的区块链，目的是对读取权限或者对外开放权限进行限制。

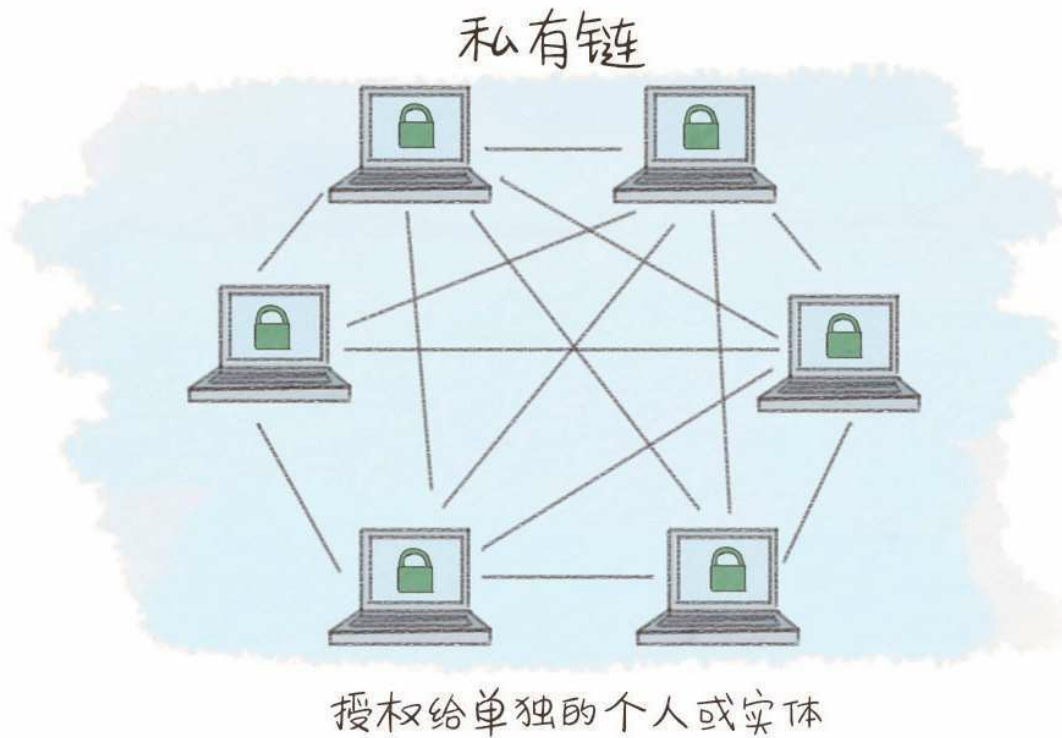


图2 - 75 区块链的私有链

私有链有如下几个特点：

1. 交易速度非常快

私有链中少量的节点具有很高的信任度，并不需要每个节点都来验证一个交易。因此，私有链的交易速度比公有链快很多。

2. 为隐私提供更好的保障

私有链的数据不会被公开，不能被拥有网络连接的所有人获得。

3.交易成本大幅降低甚至为零

私有链上可以进行完全免费或者至少说是非常廉价的交易。如果一个实体机构控制和处理所有的交易，它就不再需要为工作收取费用。

4.有助于保护其基本的产品不被破坏

银行和传统的金融机构使用私有链可以保证它们的既有利益，以至原有的生态体系不被破坏。

三、联盟链

联盟链是指其共识过程受到预选节点控制的区块链。例如，对由15个金融机构组成的共同体而言，每个机构都运行着一个节点，为了使每个区块生效需要获得其中半数以上也就是8家机构的确认。区块链可能会允许每个人读取，也可能会受限于参与者走混合路线。[\[15\]](#)

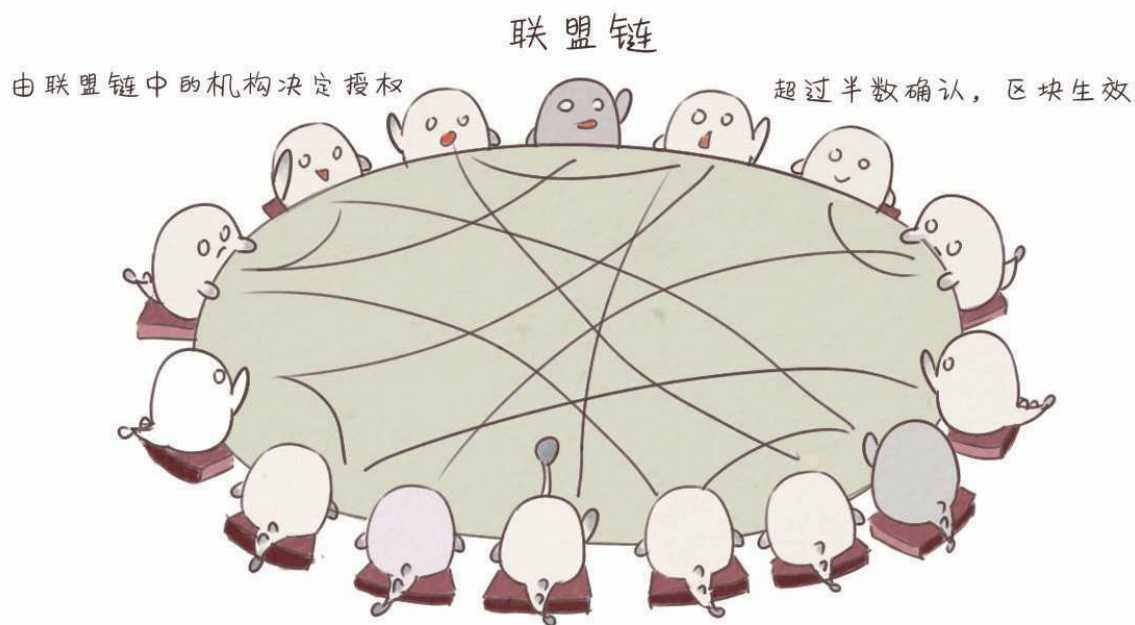


图2-76 区块链的联盟链

联盟链可以视为“部分去中心化”，区块链项目R3 CEV就可以认为是联盟链的一种形态。

四、其他的说法

我们再来说说区块链分类中的其他几种说法——许可链、混合链和复杂链。

许可链是指每个节点都需要许可才能加入的区块链系统，私有链和联盟链都属于许可链。随着区块链技术的日益发展，区块链的技术架构不再简单地划分为私有链和公有链，它们之间的界限越来越模糊，于是复杂链和混合链的概念就逐渐被人提出来了。

区块链的发展脉络

根据区块链科学研究所创始人梅兰妮·斯万（Melanie Swan）的观点，区块链技术发展分三个阶段或领域：区块链1.0、区块链2.0和区块链3.0。[\[16\]](#)

区块链1.0：以比特币为代表的可编程货币。它更多是指数字货币领域的创新，如货币转移、兑付和支付系统等。

区块链2.0：基于区块链的可编程金融。它更多涉及一些合约方面的创新，特别是商业合同以及交易方面的创新，比如股票、证券、期货、贷款、清算结算、所谓的智能合约等。

区块链3.0：区块链在其他行业的应用。它更多地对应人类组织形态的变革，包括健康、科学、文化和基于区块链的司法、投票等。



图2-77 区块链的发展脉络

区块链的共识机制

我们在了解共识机制之前，先来看两个古老的引入问题，类两军问题和拜占庭将军问题。

问题一：类两军问题

说到这个问题，网络上广为流传的解释如下：

有两个相距很远的军队要传递信息，蓝军派遣一个信使去跟红军说：“有本事把意大利炮拿出来！”红军收到信息后又派了一个信使去跟蓝军说：“收到指令！”然后蓝军又派一个信使去跟红军说：“知道你收到指令了！”然后红军又派一个信使去跟蓝军说：“知道你知道我收到指令了！”然后蓝军又派一个信使去和红军说：“知道你知道我知道你收到指令了！”然后就没完没了了。



图2-78 类两军问题

问题二：拜占庭将军问题

拜占庭将军问题是一个很古老的问题，具体阐述如下：

拜占庭罗马帝国在军事行动中，采取将军投票的策略来决定是进攻还是撤退，也就是说如果多数人决定进攻，就冲上去。但是军队中如果有奸细（比如将军已经反水故意乱投票，或者传令官叛变擅自修改军令），那怎么保证最后投票的结果真实反映了忠诚的将军的意愿呢？[\[17\]](#)

我们详细说明一下这个问题。

在很久很久以前，有一个强大的帝国叫作拜占庭，它的军队非常强大，周围有10个小国家，饱受拜占庭帝国的欺压，但是，必须同一时间有6个以上的国家进攻才有可能打败拜占庭帝国，否则就一定会战败。

这个时候，问题就出现了，古时候军队之间的通信完全依赖于人，如果一个国家的军队里有奸细，无论是下令的将军还是传信的通信兵，都可能会使得另外9个国家收到假消息，从而造成作战失败。那么，如果你是其中一个小国的国王，你该如何判断一定会有另外5个以上的国家与你并肩作战呢？毕竟一个不小心，你就亡国了。

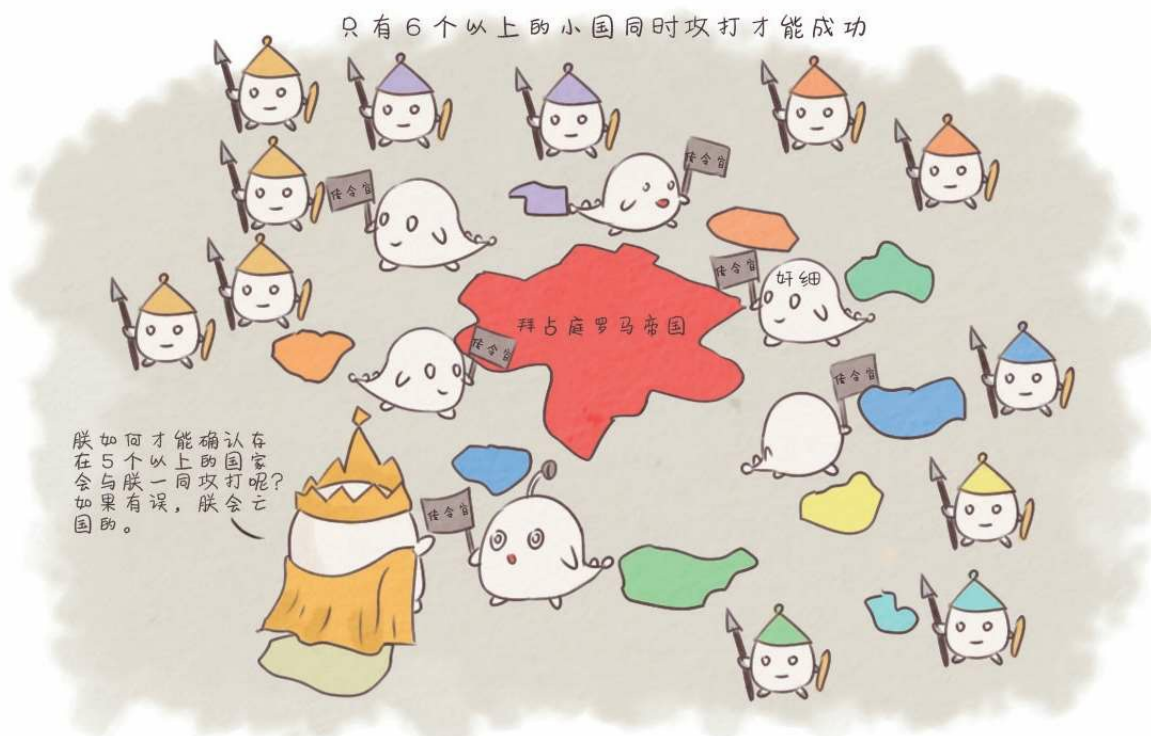


图2-79 拜占庭将军问题

正是由于以上这些问题，我们需要达成共识。区块链上的共识机制有多种，没有一种共识机制是完美无缺的，同时也意味着没有一种共识机制是适合所有应用场景的。这里我们引用了“张童鞋”的一篇文章，并获得了他的授权。我们选取了其中比较有特点的9种共识机制做一个简单介绍，常见的共识机制主要有工作量证明、权益证明和股份授权证明三种。

一、工作量证明

工作量证明（Proof of Work，简称PoW）通常只能从结果证明，因为监测工作过程通常是烦琐且低效的。

比特币在区块的生成过程中使用了PoW机制，一个符合要求的区块哈希值由N个前导零构成，零的个数取决于网络的难度值。要得到合理的区块哈希值需要经过大量的尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的区块哈希值，说明该节点确实经过了大量的尝试计算，当然，这并不能得出计算次数的绝对值，因为寻找合理的哈希值是一个概率事件。当节点拥有占全网n%的算力时，该节点即有n%的概率找到区块哈希值。

PoW依赖机器进行数学运算来获取记账权，资源消耗大、共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网50%节点出错。

PoW的优点：完全去中心化，节点自由进出。

PoW的缺点：目前比特币已经吸引全球大部分的算力，其他再使用PoW共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长。

使用PoW的项目有：比特币、以太坊前三个阶段——Frontier（前沿）、Homestead（家园）、Metropolis（大都会）。以太坊的第4个阶段，即Serenity（宁静），将采用权益证明机制。

二、权益证明

权益证明（Proof of Stake，简称PoS）由“Quantum Mechanic”2011年在比特币论坛讲座上首先提出，后经Peercoin（点点币）和NXT（未来币）以不同思路实现。

PoS的主要理念是节点记账权的获得难度与节点持有的权益成反

比，相比PoW，其在一定程度上减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算，竞争获取记账权的方式，可监管性弱。该共识机制的容错性和PoW相同。它是PoW的一种升级，根据每个节点所占地币的比例和时间，等比例地降低挖矿难度，从而加快找到随机数的速度。

在PoW中，一个用户可能拿1 000美元来购买计算机，并加入网络来挖矿以此产生新区块，从而得到奖励。而在PoS中，用户可以拿1 000美元购买等价的代币，并把这些代币当作押金放入PoS机制中，这样用户就有机会产生新区块而得到奖励。

总体而言，这个系统中存在一个持币人的集合，他们把手中的代币放入PoS机制中，这样他们就变成验证者。比如对区块链最前面的一个区块而言，PoS算法在验证者中随机选取一个（选择验证者的权重依据他们投入的代币量，比如一个投入押金为10 000代币的验证者被选择的概率是一个投入1 000代币验证者的10倍），给他权利产生下一个区块。如果在一定时间内，这个验证者没有产生一个区块，则选出第二个验证者代替产生新区块。与PoW一样，PoS以最长的链为准。

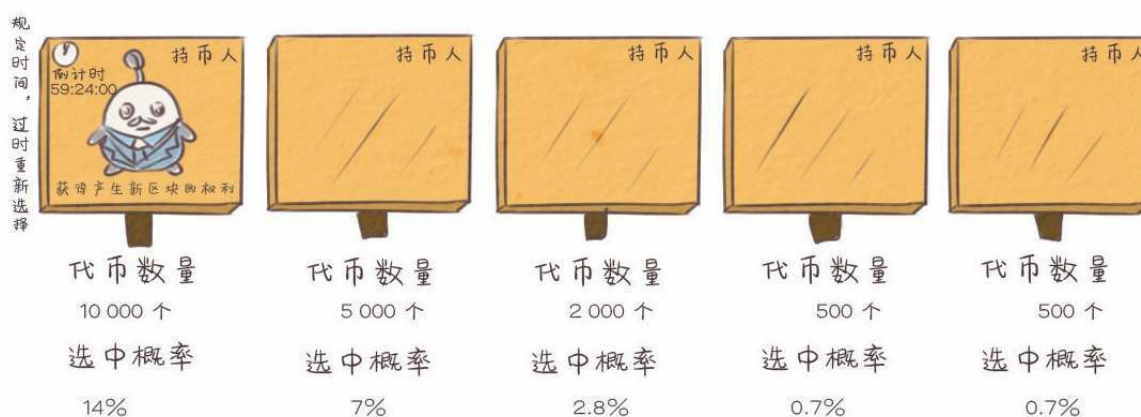


图2 - 80 PoS算法随机选取

随着规模经济（指扩大生产规模引起经济效益增加的现象）的消失，中心化所带来的风险减小了。价值1 000万美元的代币带来的回报不多不少，是价值100万美元代币的10倍，不会有人因为负担得起大规模生产工具而得到不成比例的额外回报。

PoS的优点：在一定程度上缩短了共识达成的时间；不再需要大量消耗能源去挖矿。

PoS缺点：还是需要挖矿，本质上没有解决商业应用的痛点；所有的确认都只是一个概率上的表达，而不是一个确定性的事情，理论上有可能存在其他攻击影响，例如，以太坊的DAO攻击事件造成以太坊硬分叉，而ETC随之出现，事实上证明了此次硬分叉的失败。

三、股份授权证明

BitShares（比特股）社区首先提出了股份授权证明（简称**DPoS**）机制，它与**PoS**的主要区别在于节点选举若干代理人，由代理人验证和记账，但其合规监管、性能、资源消耗和容错性与**PoS**相似。类似于董事会投票，持币者投出一定数量的节点，进行代理验证和记账。

DPoS的工作原理如下：每个股东按其持股比例拥有相应的影响力，51%股东投票的结果将是不可逆且有约束力的，其挑战是通过及时而高效的方法达到“51%批准”。为了达到这个目标，每个股东可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每位代表分配到一个时间段来生产区块。

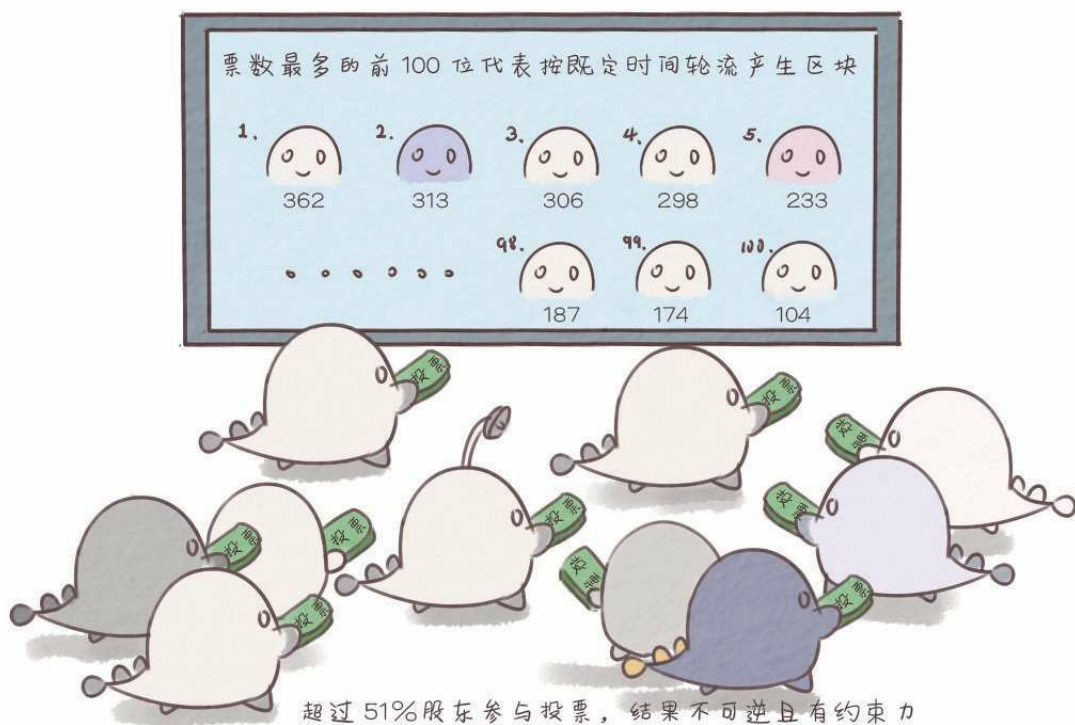


图2-81 DPoS工作原理

所有的代表将收到等同于一个平均水平的区块所含交易费的10%作为报酬。如果一个平均水平的区块用100股作为交易费，一位代表将获得一股作为报酬。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这不太可能发生，因为制造该区块的代表可以与制造该区块前后的区块的代表建立直接连接。建立这种与你之后的代表（也许也包括其后的那名代表）的直接连接是为了确保你能得到报酬。

DPoS的投票模式可以每30秒产生一个新区块，并且在正常的网络条件下，区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。执行该模式的基本步骤如下：

1. 成为代表。成为一位代表，你必须在网络上注册你的公钥，并获得一个32位的特有标识符。该标识符会被每笔交易数据的“头部”引用。

2. 授权投票。每个钱包有一个参数设置窗口，在该窗口里用户可以选择一位或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建专门以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。

3. 保持代表诚实。每个钱包将显示一个状态指示器，让用户知道他们的代表表现如何。如果他们错过了太多的区块，那么系统将会推荐用户更换一位新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一位新代表。

4. 抵抗攻击。在抵抗攻击上，前100位代表所获得的权力是相同的，即每位代表都有一项平等的投票权，因此，无法通过获得超过1%的选票而将权力集中到单一代表上。由于只有100位代表，不难想象一个攻击者可以对每位轮到其生产区块的代表依次进行拒绝服务攻击。幸运的是，由于每位代表的标识是其公钥而非IP地址，这种特定攻击的威胁很容易被减轻。这将使确定DDoS（分布式拒绝服务）攻击目标更为困难。而代表之间的潜在连接将使妨碍他们生产区块变得更为困难。

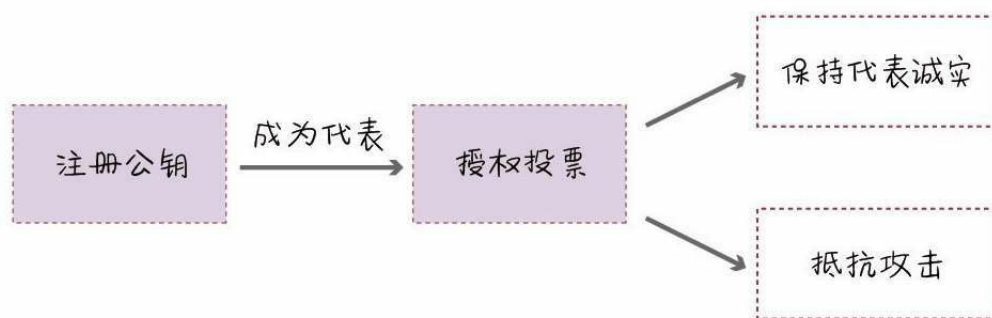


图2 - 82 DPoS的投票模式

DPoS的优点：大幅缩小参与验证和记账节点的数量，可以达到秒

级的共识验证。

DPoS的缺点：整个共识机制还是依赖于代币，而很多商业应用是不需要代币的。

四、投注共识

投注共识是以太坊下一代的共识机制Casper（鬼马小精灵）引入的一个全新概念，属于PoS。Casper的共识是按区块达成的，而不是像PoS那样按链达成。

为了防止验证人在不同的世界中提供不同的投注，我们还有一个简单严格的条款：如果你两次的投注序号一样，或者说你提交了一个无法让Casper依照合约处理的投注，你将失去所有保证金。从这一点我们可以看出，Casper与传统的PoS不同的是，Casper有惩罚机制，这样非法节点通过恶意攻击网络不仅得不到交易费，而且还面临着保证金被没收的风险。

Casper协议下的验证人需要完成出块和投注两个活动。具体如下：

出块是一个独立于其他所有事件而发生的过程，验证人收集交易，当轮到他们的出块时间时，他们就制造一个区块，并签名，然后发送到网络上。投注的过程更为复杂一些，目前Casper默认的验证人策略被设计为模仿传统的拜占庭容错共识：观察其他的验证人如何投注，取33%处的值，向0或者1进一步移动。

而客户端确认当前状态的过程是这样的：一开始先下载所有的区块和投注，然后用上面的算法来形成自己的意见，但是不公布意见；它只要简单地按顺序在每个高度进行观察，如果一个区块的概率高于0.5就处理它，否则就跳过它。在处理所有的区块之后所得到的状态就可以显示为区块链的“当前状态”。客户端还可以给出对于“最终确定”的主观看

法：如果高度k之前的每个区块形成的意见高于99.999%或者低于0.001%，那么客户端就可以认为前k个区块已经最终确定。

五、瑞波共识机制

瑞波共识算法使一组节点能够基于特殊节点列表形成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由该俱乐部51%的会员投票通过。共识遵循这些核心成员的“51%权力”，外部人员则没有影响力。由于该俱乐部由中心化开始，它将一直是中心化的，而如果它开始腐化，股东们什么也做不了。与比特币及Peercoin一样，瑞波系统将股东们与其投票权隔开，因此，它比其他系统更中心化。

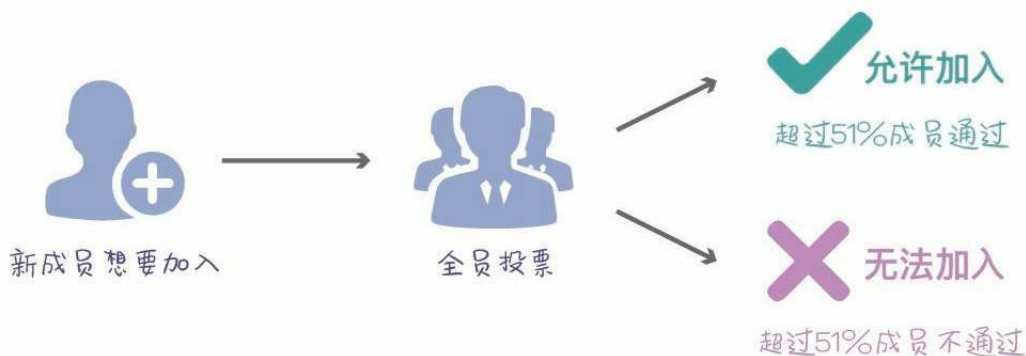


图2-83 瑞波共识机制

六、Pool验证池

基于传统的分布式一致性技术以及数据验证机制，Pool（联营）验证池是目前行业内大范围使用的共识机制。它的优缺点如下。

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Paxos、Raft）的基础上，实现秒级共识验证。

缺点：去中心化程度不如比特币，更适合多方参与的多中心商业模

式。

七、实用拜占庭容错

在分布式计算上，不同的计算机通过信息交换尝试达成共识，但有时候，系统中的协调计算机或成员计算机可能因系统错误交换错的信息，以致影响最终的系统一致性。对于拜占庭将军问题，若根据错误计算机的数量，寻找可能的解决办法，这其实无法找到一个绝对的答案，只可以用来验证一个机制的有效程度。

而拜占庭将军问题的可能解决方法为：在 $N \geq 3F + 1$ 的情况下，一致性是可能实现的（ N 为计算机总数， F 为有问题的计算机总数）。信息在计算机间互相交换后，各计算机列出所有得到的信息，以大多数的结果作为解决办法。

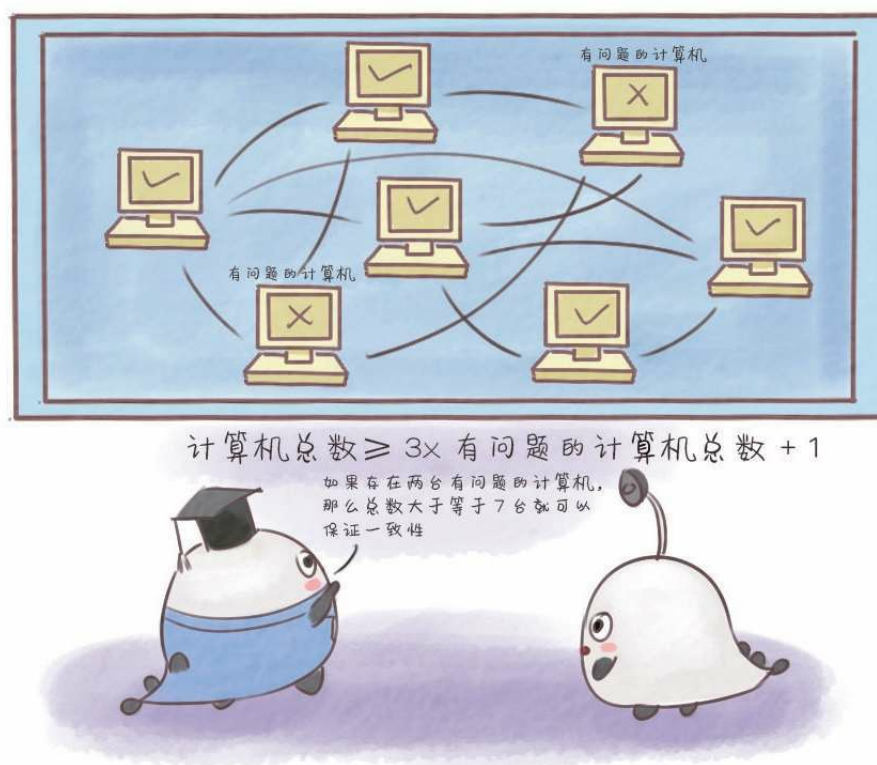


图2 - 84拜占庭容错

最早由卡斯特罗和利斯科夫在1999年提出的实用拜占庭容错（PBFT）是第一个得到广泛应用的拜占庭容错算法。只要系统中有2/3的节点是正常工作的，就可以保证一致性。

实用拜占庭容错算法的总体过程如下：客户端向主节点发送请求调用服务操作，如“<REQUEST,o,t,c>”，这里客户端c请求执行操作o，时间戳t用来保证客户端请求只会执行一次。每个由副本节点发给客户端的消息都包含了当前的视图编号，使得客户端能够追踪视图编号，从而进一步推算出当前主节点的编号。客户端通过点对点消息向它自己认为的主节点发送请求，然后主节点自动将该请求向所有备份节点进行广播。

视图编号是连续编号的整数。主节点由公式 $p = v \bmod |R|$ 计算得到，这里v是视图编号，p是副本编号，|R|是副本集合的个数。

副本发给客户端的响应为“<REPLY,v,t,c,i,r>”，v是视图编号，t是时间戳，i是副本的编号，r是请求执行的结果。

主节点通过广播将请求发送给其他副本，然后就开始执行三个阶段的任务。

1.预准备阶段。主节点分配一个序列号n给收到的请求，然后向所有备份节点群发预准备消息，预准备消息的格式为“<<PRE-PREPARE,v,n,d>,m>”，这里v是视图编号，m是客户端发送的请求消息，d是请求消息m的摘要。

2. 准备阶段。如果备份节点i接受了预准备消息，则进入准备阶段。在准备的同时，该节点向所有副本节点发送准备消息“<PREPARE,v,n,d,i>”，并且将预准备消息和准备消息写入自己的消息日志。

3. 确认阶段。当“(m,v,n,i)”条件为真的时候，副本i将“<COMMIT,v,n,D(m),i>”向其他副本节点广播，于是就进入了确认阶段。所有副本都执行请求并将结果发回客户端。客户端需要等待不同副本节点发回相同的结果，作为整个操作的最终结果。

如果客户端没有在有限时间内收到回复，请求将向所有副本节点进行广播；如果该请求已经在副本节点处理过了，副本就向客户端重发一遍执行结果；如果请求没有在副本节点处理过，该副本节点将把请求转发给主节点；如果主节点没有将该请求进行广播，那么就认为主节点失效；如果有足够多的副本节点认为主节点失效，则会触发一次视图变更。

图2-85展示了在没有发生主节点失效的情况下算法的正常执行流程，其中副本0是主节点，副本3是失效节点，而c是客户端。

实用拜占庭容错机制是一种采用“许可投票、少数服从多数”来选举领导者并进行记账的共识机制，该共识机制允许拜占庭容错，允许强监管节点参与，具备权限分级能力，性能更高，耗能更低，而且每轮记账都会由全网节点共同选举领导者，允许33%的节点作恶，容错性为33%。由于特别适合联盟链的应用场景，实用拜占庭容错机制及其改进算法为目前使用最多的联盟链共识算法，其改进算法在以下方面进行了调整：修改底层网络拓扑的要求，使用P2P网络；可以动态地调整节点数量；减少协议使用的消息数量。

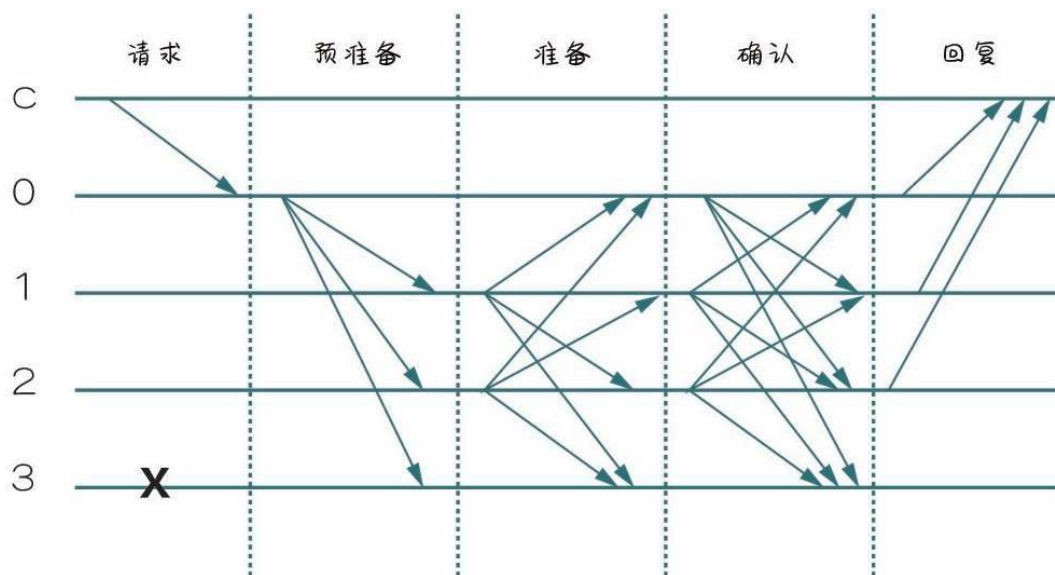


图2-85 未发生主节点失效的情况下的算法

八、授权拜占庭容错

2016年4月，小蚁公司发布共识算法白皮书，描述了一种通用的共识机制——授权拜占庭容错，提出了一种改进的拜占庭容错算法，使其能够适用于区块链系统。授权拜占庭容错算法在实用拜占庭容错算法的基础上进行了以下改进：

1. 将C/S（客户机/服务器）架构的请求响应模式改进为适合P2P网络的对等节点模式；
2. 将静态的共识参与节点改进为可动态进入、退出的共识参与节点；
3. 为共识参与节点的产生设计了一套基于持有权益比例的投票机制，通过投票决定共识参与节点（记账节点）；
4. 在区块链中引入数字证书，解决了投票中对记账节点真实身份的

认证问题。

授权拜占庭容错机制的优点：专业化的记账人；可以容忍任何类型的错误；记账由多人协同完成；每一个区块都有最终性，不会分叉；算法的可靠性有严格的数学证明。

授权拜占庭容错机制的缺点：当1/3及以上的记账人停止工作后，系统将无法提供服务；当1/3及以上的记账人联合作恶，且其他所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据。

总而言之，授权拜占庭容错机制最核心的一点，就是最大限度地确保系统的最终性，使区块链能够适用于真正的金融应用场景。

九、帕克索斯算法

这是一种传统的分布式一致性算法，是一种基于选举领导者的共识机制。领导者节点拥有绝对权限，并允许强监管节点参与，其性能高，资源消耗低。所有节点一般有线下准入机制，但选举过程中不允许有作恶节点，不具备容错性。

[1] 如何向你的“弱智室友”解释区块链？ [EB/OL]. (2016-08-08) [2017-05-18]. <http://mt.sohu.com/20160808/n463044051.shtml>.

[2] 黄峰亮。浅析比特币系统原理 [J]. 数字化用户, 2014 (5).

[3] 杨晓晨, 张明. 比特币: 运行原理、典型特征与前景展望[J]. 金融评论, 2014(2).

[4] 唐文剑, 吕雯。区块链将如何重新定义世界 [EB/OL]. (2017-02-24) [2017-05-18]. <http://www.jianshu.com/p/89275ffca97b>.

[5] 蚊子吃青蛙。公钥和私钥[EB/OL]. (2013-01-09) [2017-05-18]. <http://www.cnblogs.com/wenzichiqingwa/archive/2013/01/09/2853188.html>.

[6] 蚊子吃青蛙。公钥和私钥[EB/OL]. (2013-01-09) [2017-05-18]. <http://www.cnblogs.com/wenzichiqingwa/archive/2013/01/09/2853188.html>.

[7] 区块链运行原理[EB/OL]. (2017-03-14) [2017-05-18].

<http://www.51jrit.com/news/detail/5821>.

[8] 比特股（BTSX）投资白皮书V1.1[EB/OL]. (2014-09-16) [2017-05-18].
<http://www.docin.com/p-924681871.html>.

[9] 比特币技术帖：什么是共识、分叉、兼容性？ [EB/OL]. (2016-10-11) [2017-05-18].
<http://business.sohu.com/20161011/n469963760.shtml>.

[10] 硬分叉扩容不能保证100%一定不分裂，而软分叉可以 [EB/OL]. (2016-10-09) [2017-05-18]. <http://8btc.com/thread-40509-1-1.html>.

[11] 比特币遭遇成长之痛是解决拥堵还是彻底分裂？ [EB/OL]. (2017-03-21) [2017-05-18].
http://forex.cngold.org/c/2017-03-21/c4886602_2.html.

[12] 区块链技术详解[EB/OL]. (2017-02-15) [2017-05-18].
<https://wenku.baidu.com/view/1321bb5e326c1eb91a37f111f18583d049640f3f.html>.

[13] 区块链技术从初级到深入介绍 [EB/OL]. (2016-06-15) [2017-05-18].
http://8btc.com/thread-34731-1-1.html?utm_source=tuicool&utm_medium=referral.

[14] 全面认识区块链：公有链vs私有链[EB/OL]. (2016-08-09) [2017-05-18].
<http://www.weiyangx.com/199778.html>.

[15] 黄步添. 区块链形态[EB/OL]. [2017-05-18]. <https://wenku.baidu.com/view/43d83e1b9ec3d5bbfc0a74be.html>.

[16] 区块链来了，未来注定将颠覆我们的生活 [EB/OL]. (2016-04-20) [2017-05-18].
<http://mt.sohu.com/20160420/n445253975.shtml>.

[17] 数据阳光。从技术角度看区块链[EB/OL]. (2016-10-17) [2017-05-18].
<http://sanwen.net/a/unmoipo.html>.

03 人物篇

微秒而逝，但他们成就历史

区块链行业作为一个21世纪的风口行业，可以说是“江山代有才人出，各领风骚数百年”。这一章我们将选取几个有特点和代表性的人物，向大家讲述区块链行业中的人和他们的故事。

当然，在人物选取方面，我们争论了很久，从最初的20人到最后的5个人，我们经过了无数次的讨论，最终，我们选择了一些或许不是最著名，但相对来说最有特色的人来填充这一章。

一位是不可不提的传奇人物中本聪；一位是区块链技术领域的先行者和开拓者，发明了智能合约的尼克·萨博；另两位是有鲜明性格特点的意见领袖，在《纽约时报》撰写关于比特币的专栏的男子马克·安德森以及从华尔街走出的神奇女子布莱斯·马斯特；最后一位是区块链行业的投资大亨巴里·希尔伯特。

永远的背影：中本聪的99种传说

说起区块链行业里的传奇人物，不提这位肯定是说不过去的，他就是中本聪——比特币的创造者，可以说区块链的核心理论就是他发明的。打个稍微夸张的比喻：上帝创世的时候说“要有光”，于是世界便有了光；中本聪对着计算机屏幕敲啊敲，然后大喊一声“出现吧，我的比特币”，于是便有了比特币及其背后的区块链技术。



图3-1 中本聪

这位传奇人物不仅有才还很有意思，明明有才华却偏偏要靠性格吃饭，把神秘主义的原则诠释得彻彻底底，比特币发展初期的时候，他甚至匿名参与指导。后来比特币和区块链越来越火，中本聪却完全隐身了，既不动用自己手里价值十几亿美元的比特币，也不去申请专利，就

连提名诺贝尔经济学奖候选人都没能让他现身。

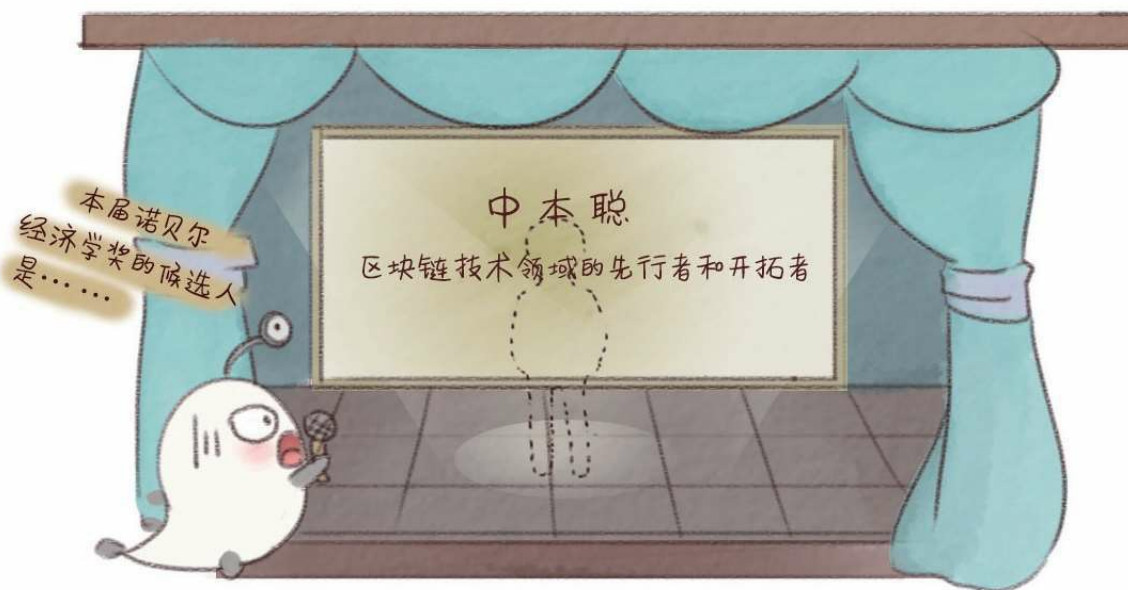


图3-2 诺贝尔经济学奖候选人

不过，不管他究竟是谁，什么时候出现，此生还会不会出现，他都实现了我小时候大声喊出的梦想——“我要改变世界”“我要成为世界未解之谜”。下面我们就来具体讲讲这位传奇人物的传奇经历。

传说中的中本聪被描绘成一个集经济学家、数学家、密码学家以及顶级黑客为一体的人物，他的传奇历史始于2008年11月1日，这一天，他发表了一篇论文《比特币：一种点对点的电子现金系统》，之后他又把理论付诸实践，在2009年1月4日创造了比特币世界的第一个区块，我们称之为“创世区块”，同年1月11日，他开发了一个客户端，其名称非常朴素——比特币客户端0.1版，召唤各路小伙伴们一起玩耍。

故事慢慢演化，比特币终于有了第一笔交易，比特币有汇率了，比特币的技术爱好者有聊天室了，比特币挖矿难度调整了，比特币被某个国家的法律认可了，比特币市值近400亿美元（按2017年5月数据估算）

.....当然，比特币的成长过程中也伴随着一些“负能量”，诸如比特币暴涨、暴跌，比特币被盗、被告。总之，比特币的历史精彩纷呈，我们会在后面详细阐述。

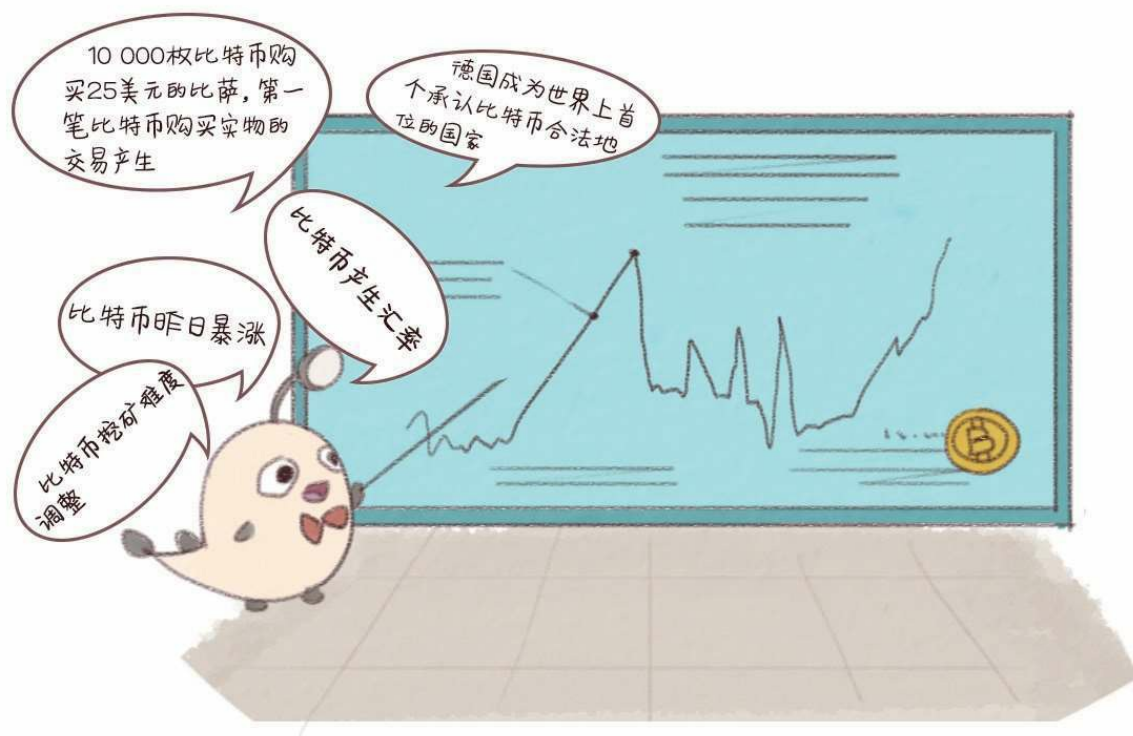


图3-3 比特币的历史精彩纷呈

在这些事件中，中本聪扮演着一个什么角色呢？事件创造者。为什么这么说？因为他消失了，全世界都没人见过中本聪，也没有人听过他的声音，FBI（美国联邦调查局）和全世界的媒体都在找他，但是谁也没找到，大家都能看到2008年比特币创始初期他在论坛、邮箱、网站主页的发言，针对这些看似线索的发言的探究到最后都被逼入了死胡同。



图3-4全世界寻找中本聪

比特币的历史上好几次大事件都是因为“中本聪”这个名字引起的，比如人们发现一个日本人是中本聪，随后又发现一个澳大利亚人是中本聪，《纽约时报》声称找到了中本聪本人。最近的一次轰动，是由一位澳大利亚企业家克雷格·史蒂芬·赖特引起的，他通过BBC（英国广播公司）、《经济学人》和《智族》宣布，自己就是如假包换的比特币创始人中本聪，并展示了一笔发生在2009年1月的交易，中本聪向帮助构建比特币协议的程序员之一哈尔·芬尼转账了10枚比特币，这是有史以来第一笔比特币系统内的转账交易。同时，他还向英国提交了50多项围绕比特币和其底层区块链技术的专利申请。



图3-5 中本聪的身份疑云

大家觉得这下终于找到中本聪了，纷纷前去围追堵截，抢专访上头条。一个转折性的事件又发生了，在《连线》刊登的相关文章引起轩然大波的48小时之后，这一轮身份风波被中本聪的邮件平息了，中本聪在邮件中淡定地说道：“我不是克雷格·赖特，我们每个人都是中本聪。”

其实，要证明自己是中本聪也很简单，比特币的本质是一个分布式账本，可以说，它是一本不能修改、不能毁坏、永远不间断、所有人都可查询的账本。那么，基于分布式账本的特性，我们要怎样做身份验证呢？首先，我们使用一个比特币公钥，向外界公布，并声明这个公钥对应的私钥归你所有；然后使用私钥签名，就可以证明自己确实拥有该地址的私钥了。

倒推到中本聪身上，他要如何证明自己就是中本聪呢？只需要使用“创世区块”里的私钥对“创世区块”的公钥签名，随意使用什么签名文本都无所谓，因为“创世区块”的私钥一定为比特币的发明人所有。^[1]

现如今，比特币市值已经完美地碾压了许多国家的法定货币。多个国家都认可或者放宽了比特币的法律地位，区块链应用遍地开花，成为金融科技领域炙手可热的“新贵”。据预估，中本聪持有约100万枚比特币，同时手握无数个专利，完全是人生赢家的典型。历史上想要凭个人的力量创造一种货币的人不是没有，但是成功的却只有中本聪一人。

当然，正如中本聪所说，“我们每个人都是中本聪”，我们每个人都是区块链技术的践行者和参与者，我们期待见证被区块链技术改变后的世界。

中本聪，在各处的配图中，永远都是用一个背影来代替，但是，我们期待“每个中本聪”创造的99种传说。

当尼克·萨博被自动售货机“砸中”

牛顿被树上掉下来的“上帝的苹果”砸中，于是茅塞顿开，发明了牛顿运动定律。在区块链领域，也有这么一个人被自动售货机“砸中”，他发明了智能合约。

大家应该都知道自动售货机，这个笨头笨脑的大家伙其实非常厉害。你塞进去钱币，它就会吐出来商品。我们看不到内在的工作机制，但都知道，你不塞钱进去，就不会有东西吐出来。

说到这里，我们的话题就可以展开了。此人根据售货机的灵感，提出了智能合约的概念，他就是尼克·萨博，他是一位计算机科学家、密码学家、法律学者，是智能合约等创新概念的先驱，他还曾被人怀疑是中本聪。目前，他正在募集资金，打算建立一个区块链技术公司。



图3-6 尼克·萨博

介绍一位科学家最科学的方式就是讲述他发明的科学。我们回到开始的话题，在尼克·萨博眼中，自动售货机有着不一样的魅力，购买者向售货机投入一定数量的货币，选择要购买的商品，这就在两者间创建了一种强制执行的合约。购买者投入货币并选择商品，而卖家通过售货机内置的逻辑提供商品和找零。



图3-7 自动售货机的逻辑

如果我们投入硬币但售货机没有吐出商品，我们会认为售货机不遵守合约，有些愤怒的人甚至拳打脚踢，其实售货机也很无辜，因为它还没有识别你投入的硬币，或者你投入了一张假钞，自然没法吐出来商品啦。这其实是一种简易化的智能合约。



图3-8 简易的智能合约

我们再来看另一个例子，《怪诞心理学》提出了这样一个问题：在网上买东西，如果你付了钱，对方却没有发货，这时候如果他撒谎，说自己发货了，双方该如何自证呢？

支付宝作为第三方，确保交易双方不会存在这样的问题，你先付款到支付宝，然后商家确认发货后再打款，保障了交易双方的利益，我们可以称之为担保交易的模式。支付宝是支付工具，其背后的工作机制却与智能合约的逻辑基本一致——基于信任而产生。不过，这里也存在一个问题，如果有一天支付宝的服务器遭受不明物体入侵，整体报废了，记录也不存在了，买卖双方又无法自证了。



图3-9 支付宝的逻辑

说到这里，我们就可以引出智能合约的含义了，智能合约就是一个计算机程序，是一个任何人都可以使用的去中心化系统，不需要任何中介机构。它有几个条件：

1. 必须有货币参与。没有货币一切交易都是空谈，无论是使用法币，还是使用加密数字货币，总之，必须有货币。

2. 资产必须数字化。如何把一辆车数字化呢？答案是给它一把密码学锁。我们现在用的车都是物理锁，所以交付车实际上是交付车钥匙。想象一下，有一天车的锁变成了密码学公钥，而只有持私钥的人才能打开车。很科幻，是不是？但这是可以实现的。

3. 资产必须联网且绝对信任某个数据库。

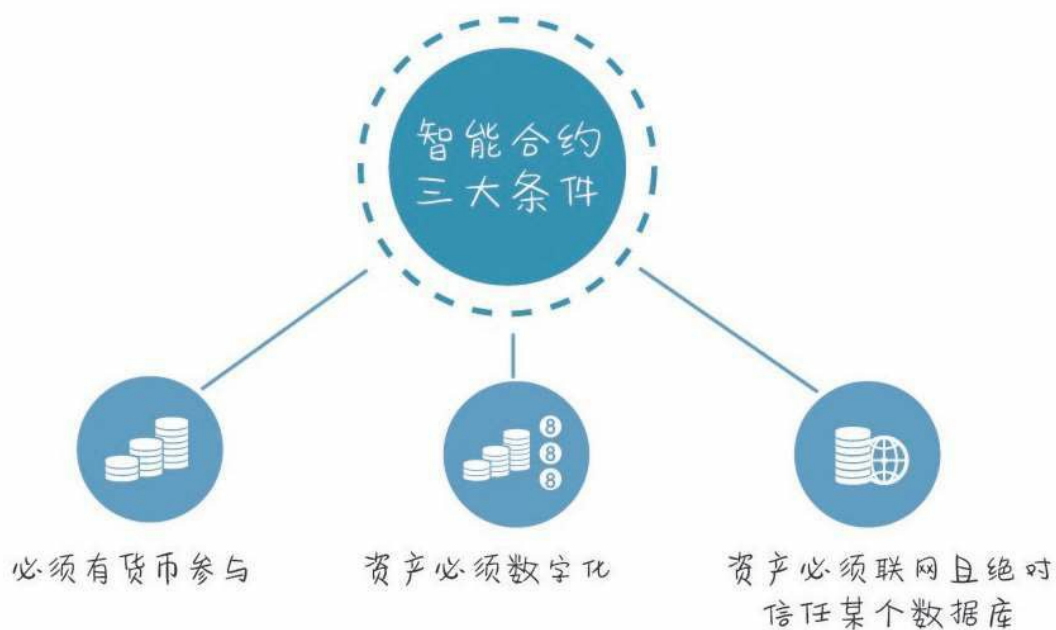


图3 - 10 智能合约的特点

从本质上讲，这些自动合约的工作原理类似于其他计算机程序的“if-then”语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。^[2]目前，瑞士联合银行、英国巴克莱银行以及美国摩根大通等金融机构都在研究把智能合约用于自动化交易结算，这种方式能大大降低成本。

智能合约利用程序算法替换执行合同，杜绝了执行主体和交易的道德风险。



图3 - 11智能合约的结构模式

等到以上三大条件都实现的时候，我们就会发现智能合约已经变得像如今的支付宝一样，你不需要知道背后的技术，但你信任它，而且你不得不使用它来完成交易。在区块链的世界里，智能合约将会无处不在。

从华尔街走出的区块链女性领袖人物

因为比特币及其背后的区块链技术天生带着一种极客的气息以及一种“尔等凡人你们看不懂夜的黑”的高傲气质，所以，区块链行业的权威和意见领袖更多是低调、不爱发表观点的男性。

但是，其中仍然有几位巾帼不让须眉的女性意见领袖，比如区块链创业公司BlockCypher的CEO（首席执行官）凯瑟琳·尼科尔森，该公司已经筹集了350万美元的资金，还有数字资产控股公司的CEO布莱斯·马斯特等。

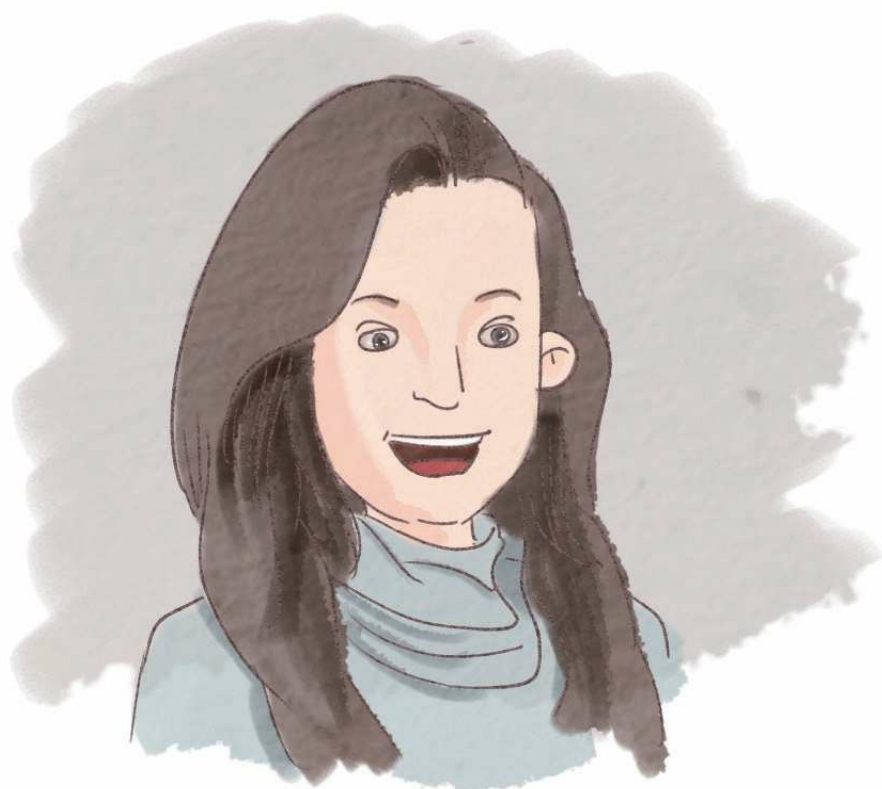


图3-12 凯瑟琳·尼科尔森

下面我们就来讲讲布莱斯·马斯特，她是摩根大通前高管，在摩根

大通待了近30年，离开摩根大通之后开始了创业之旅，她创立了数字资产控股公司并担任CEO，这是一家寻求将区块链技术应用到华尔街市场的创业公司。



图3-13 区块链的女性意见领袖

这家公司的第一个大客户就是她的前任雇主摩根大通。摩根大通现在正与数字资产控股公司合作测试使用区块链来加快结算速度。她认为，“我们将在未来一两年看到区块链技术以各种形式被部署到商业环境中。但是，这并不意味着区块链技术同时会成为主流。我认为区块链技术要想成为主流技术，需要5—10年的时间”。^[3]

目前数字资产公司已经得到了6 000万美元的融资。由于马斯特在华尔街的巨大名气，她的举动可能会促成区块链技术对传统金融行业的正向影响。

在《纽约时报》撰写专栏的男子

1971年，在美国艾奥瓦州的一个小镇上，一个小男孩降生了，谁也不知道，这个小男孩长大后将在世界上掀起的风云。他9岁开始接触计算机，在图书馆自学Basic（初学者通用符号指令代码）语言，和沃伦·巴菲特对峙，说比特币是来自火星的技术，他被誉为“互联网的点火人”。这个人就是我们要说到的第4个人物，在《纽约时报》撰写关于比特币的专栏的男子马克·安德森。



图3-14 马克·安德森



图3-15 从小自学Basic语言

我们先来简要说一下这位传奇人物的履历，马克·安德森虽然不像比尔·盖茨、乔布斯那么出名，但是他所走的每一步都和互联网的发展密切相关，我们可以从他的几次创业经历谈一谈。

在最初的十多年里，围绕在安德森身上的光环是“网景公司”——第一代浏览器的缔造者。1992年，安德森和小伙伴一起研发出了第一个加入图像元素的网页浏览器Mosaic。1993年，安德森和合伙人成立了网景公司。1995年，网景公司在纽约上市，市值一度达到29亿美元。24岁的安德森也因此在一夜之间成为亿万富翁。之后，由于IE浏览器（微软公司的网页浏览器）的兴起，1999年，网景公司被迫出手给美国在线，安德森的第一段创业经历结束了。

安德森的第二段创业经历也踩在互联网的风口上，他和合伙人创办了一家云计算公司，名为“Loudcloud”，不过2002—2006年，美国进入了互联网泡沫破裂的时代，风投公司不愿意资助互联网企业，2007年，

该公司以16亿美元的价格出售给惠普公司。

之后，安德森又加入了Facebook（脸谱网）董事会，给Twitter（推特网）当时的CEO伊万·威廉姆斯当咨询顾问，2009年，安德森和本·霍罗维茨创建了安德森-霍罗维茨风投公司。

而马克·安德森与区块链的结缘也和这家风投公司有关，安德森-霍罗维茨风投公司投资了比特币交易平台Coinbase，比特币创业公司21Inc和区块链数据商TradeBlock。当然，这些远不能成为他被列为区块链领域风云人物的有力例证。



图3-16 安德森-霍罗维茨风投公司

在区块链行业，他多以爆炸性的言论和频繁的观点输出而闻名，每次发言都引得各路媒体疯狂转载。2014年，他在《纽约时报》开设了专栏，并使用了一个大胆的标题“比特币为何重要”。他还在Twitter上随心

所欲地与自己的关注者分享与比特币和区块链相关的新闻。



图3-17 《纽约时报》专栏

2014年，投资大师沃伦·巴菲特警告投资者远离比特币，将其称为“海市蜃楼”。对此，马克·安德森回应道：“老顽固对他们不懂的新技术从来都是瞎说一通。”这次观点碰撞引发了多国媒体的疯狂转载。而安德森在接受杂志采访的时候还说过这样的观点：“比特币就像是来自火星的技术。”同时，他也在多次采访中积极回应对比特币及其背后的区块链技术的看法。



图3-18 “顶撞”巴菲特

可以说，这是一位有胆识、有魄力的意见领袖，他在比特币及区块链的对外普及中做出了很大的贡献。

想投资所有数字资产项目的大亨

接下来，我们将要讲述一位“画风清奇”的人物，闯荡江湖有一门独门绝技——“买买买”。网上时不时就会弹出这样的信息：某某区块链公司被买了，某某比特币公司被收购了，某某金融科技公司又被投资了……大多数时候，这些新闻的背后都有这样一个身影。

他就是巴里·希尔伯特，数字货币集团（DCG）的CEO。他的“采购清单”遍布全世界约20个国家，投资的公司约有60家之多。巴里·希尔伯特领导的数字货币集团是一家投资公司，而不是投资基金。



图3-19 巴里·希尔伯特

他说道：“数字货币集团拥有投资公司、收购公司以及永久持有资本的权力，我们不是一个基金，不需要把资金返还给有限合伙人，而是在公司内部重新部署资本。我们的目标是加快一个更好的金融体系的发展。”^[4]

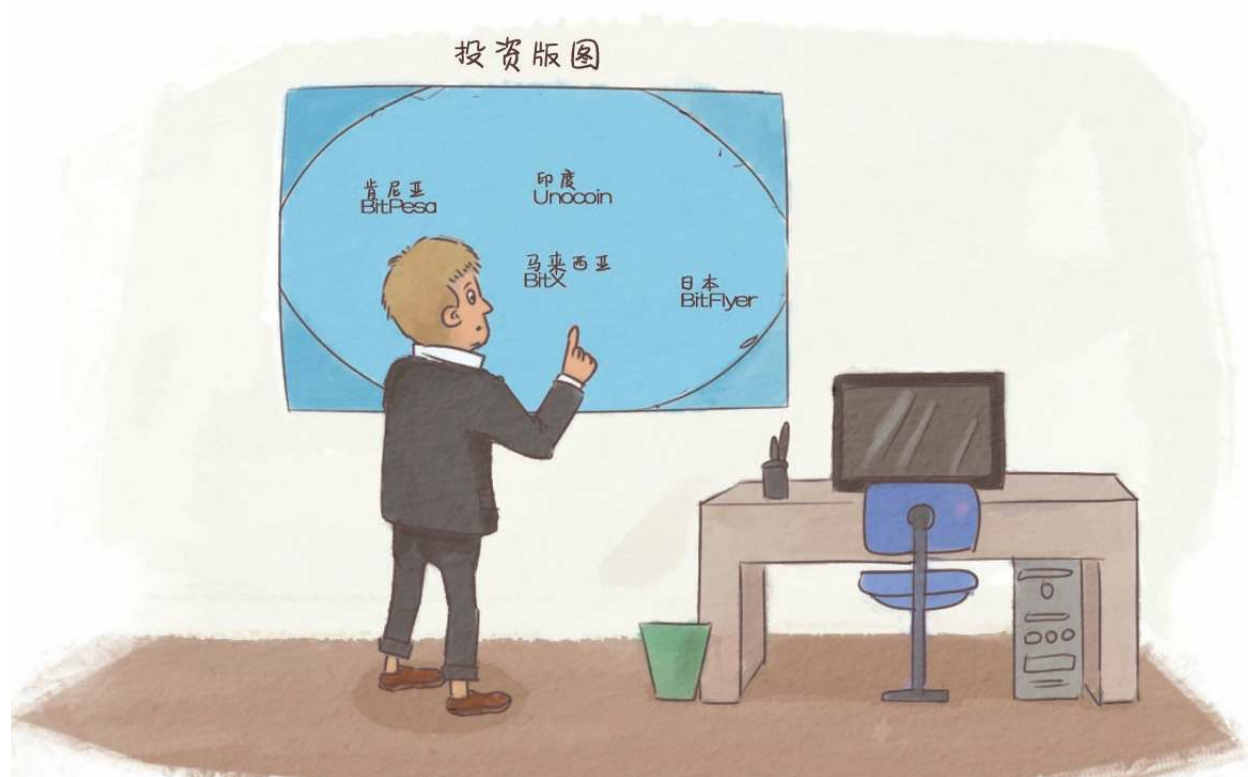


图3-20 全球投资版图

数字货币集团对区块链可谓情有独钟，投资的都是一些以区块链为重点的初创公司，早期的投资项目包括Ripple（世界上第一个开放的支付网络）、Coinbase和BitPay（比特币支付处理商）。同时，它还投资了全世界约15家比特币交易所，包括印度的Unocoin、韩国的Korbit、日本的BitFlyer、肯尼亚的BitPesa、马来西亚的BitX等，支持的币种达40余种。最近它又投资了一家利用区块链技术优化全球供应链的区块链公司Skuchain。

除了“买买买”之外，巴里·希尔伯特还是少数始终对比特币作为一种货币而感到兴奋的投资者之一，在英国“脱欧”时期，他曾表示：“比特币的表现完全可以被称为一种‘避风港资产’。”

对于各大传统金融巨头所表现的对区块链技术的热情，他表示：“我们对区块链被金融机构所采用感到很兴奋，无论它是不是比特币的区块链。但是，我们的热情依然集中在未来比特币将成为一种全球货币这件事上，这是我们的愿景。”

可以说，巴里·希尔伯特是比特币和区块链技术的“忠实信徒”，并用自己的行为“买买买”始终践行着自己坚定的信念。



图3-21 比特币的“信仰者”

[1] 真假中本聪之谜和比特币私钥签名技术[EB/OL]. (2016-07-15) [2017-05-18]. <http://zhuanlan.zhihu.com/p/21722963>.

[2] 智能合约将使我们未来不需要银行和律师 [EB/OL]. (2016-06-21) [2017-05-18].

<http://it.sohu.com/20160621/n455402402.shtml>.

[3] 巴比特。数字资产CEO: 银行将在两年内应用区块链技术, 但是成为主流需要5—10年[EB/OL]. (2016-04-07) [2017-05-18]. <http://www.8btc.com/blockchain-in-banks-a-reality>.

[4] 巴里·希尔伯特谈DCG在数字货币领域的投资策略[EB/OL]. (2016-02-01) [2017-05-18]. <http://www.okcoin.cn/t-1010622.html>.

04 应用篇

待十年后，陪你看繁花似锦

或许你第一次听到区块链这个词是因为比特币，也可能是通过某个金融科技峰会，但是，不知道你有没有发现，区块链技术发展到今天，似乎所有行业都说自己和区块链有点关系。

我们正在积极探索区块链技术，我们正在组建区块链实验室，我们的某位专家是区块链行业的“大牛”，他会带领我们用区块链的思维探索企业新的转型之路……诸如此类的话不绝于耳。似乎世界上的任何东西都能和区块链扯上关系，这究竟是抢风口还是真事实呢？

在本章中，我们将选取几个比较热门的领域和相关的案例，与大家分享一下“区块链+”这个词，看看区块链在不同领域都展现出了哪些不一样的风采。在论述中，我们将引用许多国内外的真实案例和行业专家的观点，相关的参考资料及来源我们会一一注明。

区块链+金融

如今，区块链作为一个现象级概念已经被众多政府、企业、机构认同，那么它最初是在哪里掀起“群体高潮”的呢？没错，就是金融行业。虽然说区块链技术在金融行业的应用并不成熟，目前也没有看到BAT（百度、阿里巴巴、腾讯三大互联网公司）级别的区块链金融巨头产生，但我们可以确定的是，随着越来越多的大型金融机构开展区块链项目实验并逐步取得成就，区块链必将对传统金融产生颠覆性的影响。我们甚至可以预测，区块链和大数据、人工智能一样，也是开启互联网金融新时代大门的钥匙。

在过去两年中，包括摩根大通、高盛集团、花旗银行等在内的超过20家全球顶级金融机构已经在区块链项目上投入了超过10亿美元的资金。据估计，2017年，区块链方面的投资只会更多，仅当年一年就可能超过10亿美元。

区块链+银行

在大多数国家的现有银行系统中，所有银行都是通过中央的电子账本进行账目核对的。这是一个中心化的结构，越靠近中心的机构，权限越多，储存的数据量也越多。而为了维护这个中心化系统中所有数据的准确性，银行需要付出巨大的运营成本。而凭借去中心化的特点，区块链技术可以为银行创建一个分布式的公开可查的网络，其中的所有交易数据是透明和共享的。利用区块链技术进行分布式记账可以削减无效的银行中介，节省很多运营成本。

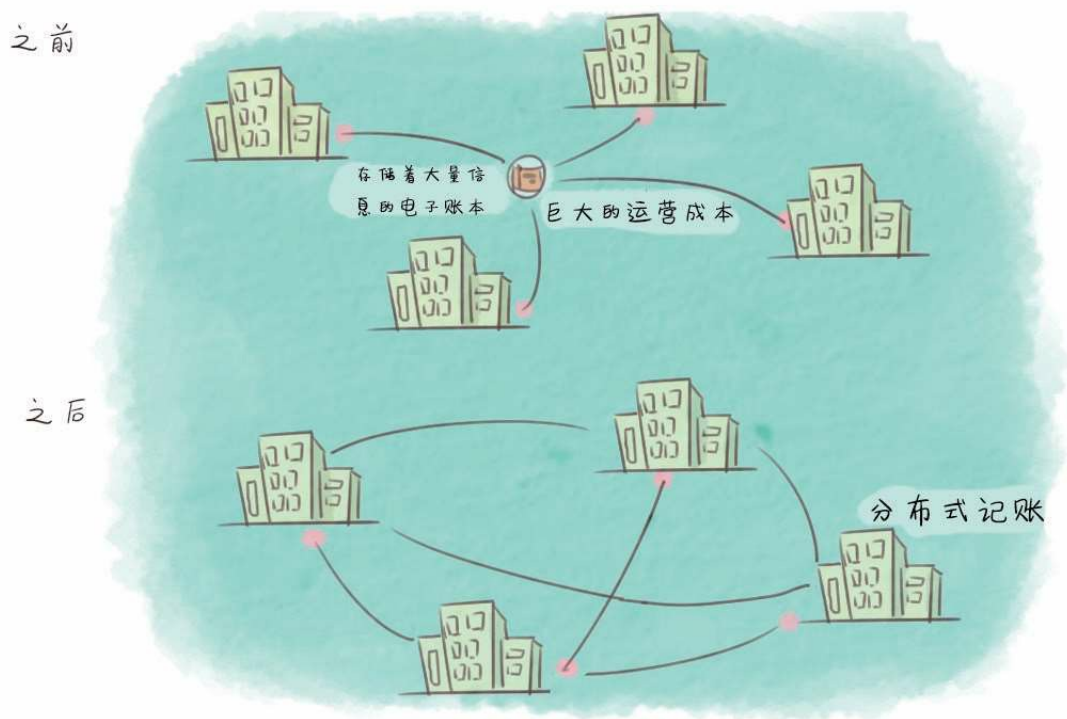


图4-1 区块链+银行

目前，区块链技术已经被许多银行认可，多家银行成立了相关的区块链实验室，致力于利用区块链技术打造一个针对银行后台的终极改造工具。一份来自西班牙的报告称，如果银行内部全都使用区块链技术，在2022年以前银行每年都能节省150亿—220亿美元的成本。

区块链+跨境支付

目前主流的传统跨境汇款方式是电汇，其汇款周期一般长达3—5个工作日，除了中间银行会收取一定的手续费，SWIFT（环球同业银行金融电讯协会）也会对通过其系统进行的电文交换收取较高的电讯费，例如在我国通过中国银行进行跨境汇款会被收取单笔150元的电讯费。

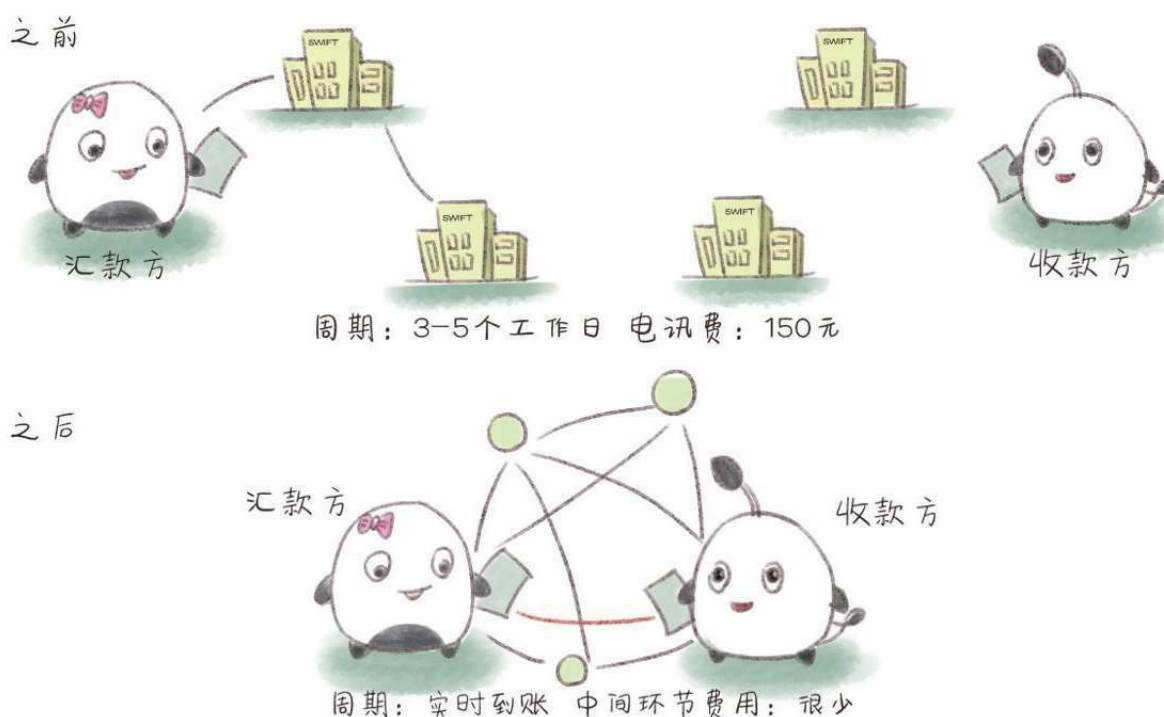


图4-2 区块链+跨境支付

而使用区块链技术可以让汇款方和收款方直接进行支付、结算，省掉了所有的中间环节费用，使跨境支付结算能够点对点地快速完成，在提高清算速度的同时还可以实现全天候支付、实时到账、提现简便且没有隐性成本。根据麦肯锡的测算，在全球范围内，区块链技术仅仅在B2B（企业对企业）跨境支付与结算业务中便可使每笔交易的成本从约26美元下降到15美元。

区块链+供应链

供应链金融，简单地说，就是银行将核心企业和上下游企业联系在一起提供灵活运用的金融产品和服务的一种融资模式，也就是把资金作为供应链的一个溶剂，增加其流动性。

在如今的供应链金融体系中，一个特定商品的供应链包括从原材料采购到制成中间产品及最终产品，最后由销售网络把产品送到消费者手中，将供应商、制造商、分销商、零售商，直到最终用户串连成一个整体。^[1]



图4-3 区块链+供应链

而区块链技术具有公开可查的特点，可以大大减少人工的介入，将目前需要纸质作业的各种流程都程序化和数字化。在区块链系统中，所有参与方都能使用一个去中心化的账本分享文件。通过智能合约，款项可以在达到预定的时间和结果时自动进行支付，在提高效率的同时，还可以在很大程度上避免人工操作的失误。根据麦肯锡的测算，在全球范围内，区块链技术在供应链金融业务中的应用能使银行减少操作风险所带来的1亿—16亿美元的损失。

区块链+信息

银行一旦建立起了自己的区块链，由于其具有不能篡改的特性，客户信息与交易记录被确认后便不受任何人为干预，也无法篡改。这有助于银行识别异常交易，防止欺诈行为的发生。

同时，银行还可以利用区块链技术建立一个分布式账本信息系统，以此检测和分析所有节点用户的交易行为，一旦有异常行为发生，系统就会发出报告，从而有效地防范欺诈、洗钱等违法行为的发生。

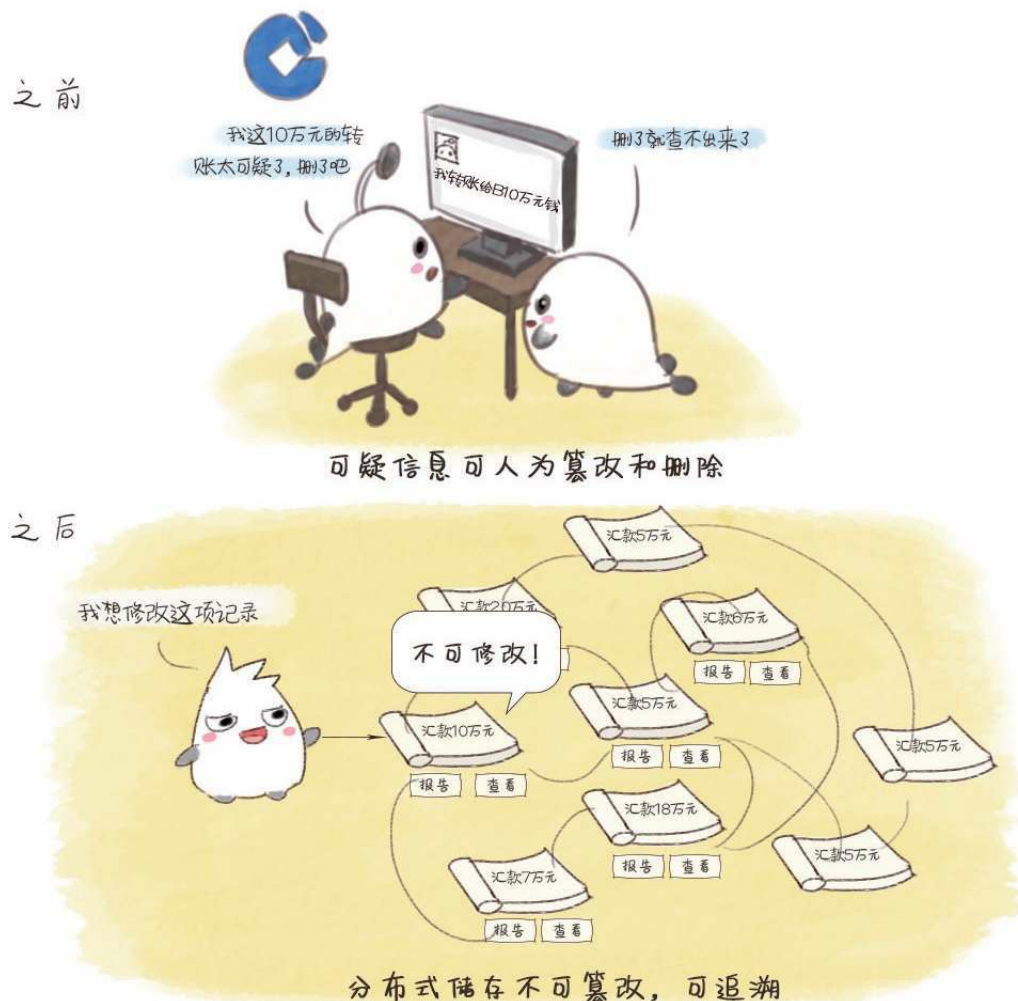


图4-4 区块链+信息

区块链+证券

在证券领域，IPO（首次公开募股）和证券交易，需要长时间的第三方参与，这就导致股票的发行与交易不仅流程长，而且成本高。而利用区块链技术，投资者和机构可以在去中心化的交易平台上自主完成IPO、自由交易，不需要任何第三方的撮合或干预，并且可以24小时不间断运作。

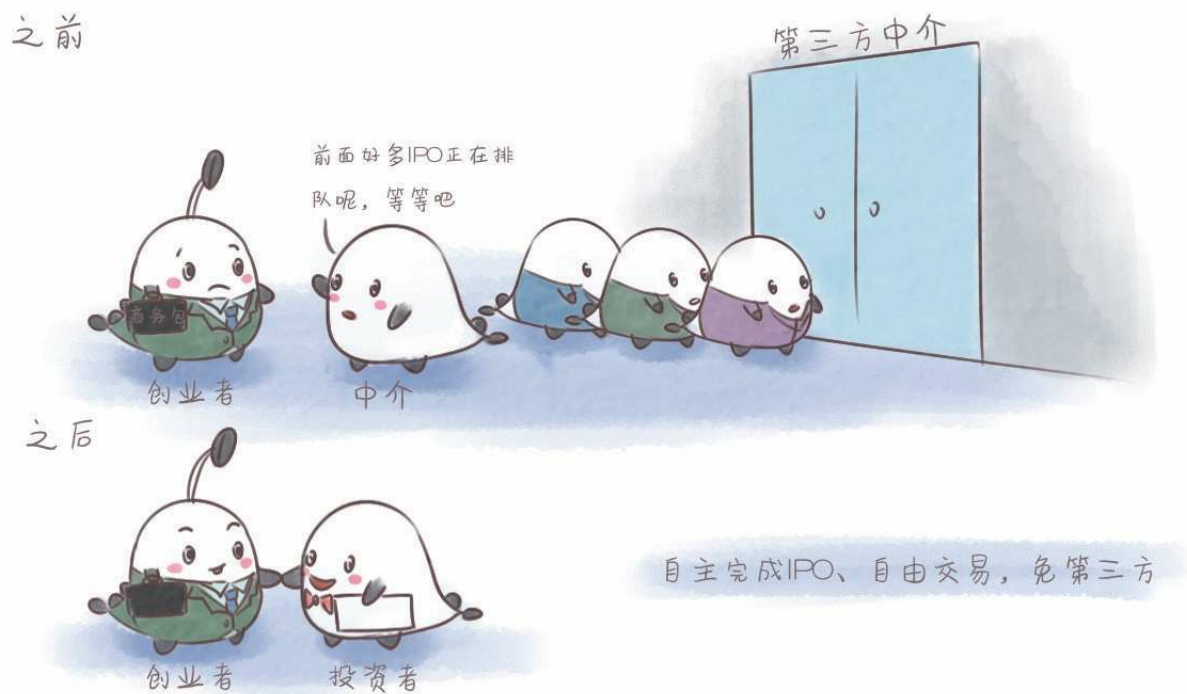


图4-5 区块链+证券

对券商及投行从业者来说，区块链的引入会使业务方向转型，弱化承销和资源获取能力，但强化为投融资客户提供专业证券咨询服务的能力。

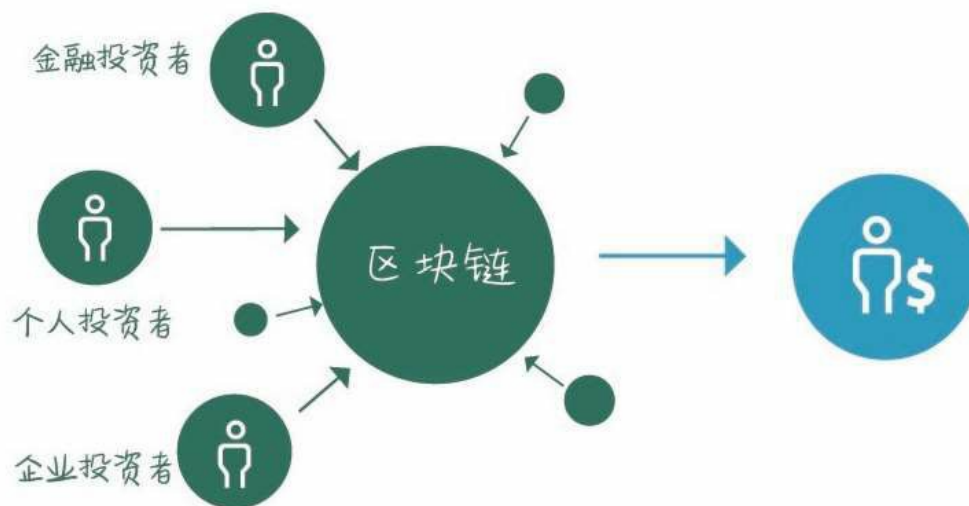


图4-6 区块链股权众筹市场

区块链+保险

在传统的保险业务中，保险机构是核心部分，全面负责资金归集、投资以及理赔，这也导致其运营和管理成本十分高昂。

但是利用区块链技术，互助保险的模式就可以变为现实。其具体操作过程是，需要出险时，参与者直接将资金支付给病患，这样就可以避免第三方机构的介入。关于资金归集和分配的一切都变得公开透明，这将降低管理成本。对于保险机构来说，它们可以转型为保险咨询公司，从而避免直接承担风险。

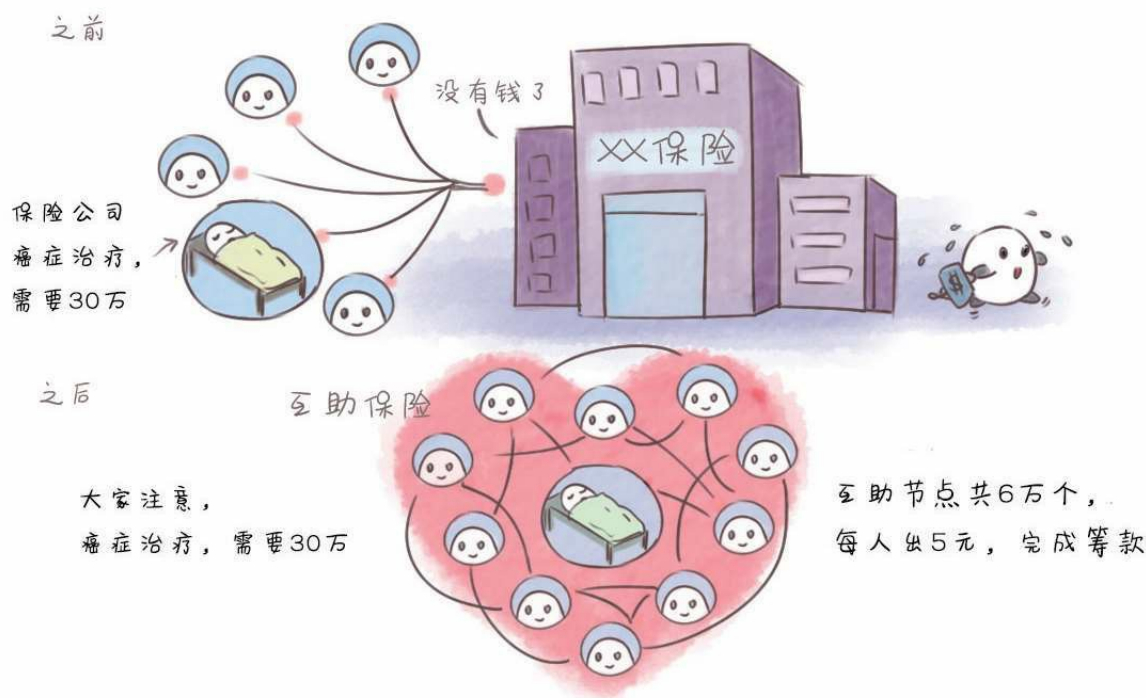


图4-7 区块链+保险

案例一：OKLink

区块链热度飙升的背后，世界各国政府、大型金融机构、企业集团纷纷投入大量资源对区块链进行研究。OKCoin币行旗下的应用OKLink是构建于区块链技术之上的新一代全球金融网络，也是中国首个商业化的区块链应用，它致力于推动全球价值传输效率，同时提升全球汇款用户体验。该应用目前已覆盖20多个国家和地区，包括中国、日本、韩国以及东南亚国家等。主要客户是全球中小型金融参与者，包括银行、汇款公司、互联网金融平台等，每月交易额达到几千万美元。



图4-8 传统汇款方式

前文已经举例说明了传统跨境汇款方式的缺点：周期长、收费高。而基于区块链技术进行跨境汇款的OKLink可以在去中心化的机制下，使用户以更低的费用和更快的速度完成跨境转账。OKLink使用区块链技术让汇款方和收款方直接进行支付、结算，省掉了所有的中间环节费用，整个网络只在中间汇率的基础上收取不超过0.5%的费用，绝无其他隐藏费用，并且保证收款人能够收到约定的金额。



图4-9 OKLink跨境汇款模式

OKLink的合作方可以对其涉及的交易进行公开查询，所有交易均可溯源。OKLink使用的区块链技术能够确保交易不可伪造和篡改，其

基于区块链打造的全球金融汇款网络可以实现支付即清算的实时结算，让国际小额汇款像发邮件一样简单、快速。

案例二：自动化对冲基金**LendingRobot Series**

位于西雅图的P2P借贷平台公司LendingRobot发布了自动化对冲基金**LendingRobot Series**。这种基金根据算法，制订了短期激进投资方案、短期保守投资方案、长期激进投资方案、长期保守投资方案等多种投资方案。

这种基金的主打特点是自动化管理，而与钱有关的、让人放心的自动化管理就一定离不开区块链这个概念。这款对冲基金每周都会发布一份详细的账本，详细到每一次交易的金额。每周的账本都有一个哈希值签名，并在以太坊区块链上获得验证，以确保数据不会被任何人篡改。

LendingRobot的首席执行官伊曼纽尔·马洛特（Emmanuel Marot）说：“所有投资者都知道‘不要把鸡蛋放在同一个篮子里’的道理，但是真的做到却不简单，因为考虑投资方案是非常伤脑筋的复杂过程，而且要求投资者对某个领域非常了解。因此我们推出了**LendingRobot Series**，通过智能控制技术和区块链技术，让了解借贷投资价值的投资者，能够放心地在我们的平台上投资。”普通对冲基金的管理费率通常为2%，此外还收取20%的业绩报酬，而LendingRobot只收取1%的资产管理费，以及最高不超过0.59%的基金运营费，而且不收取任何的业绩报酬。[\[2\]](#)

区块链+互联网管理

区块链技术在互联网安全管理及认证等领域也有很大的优势，被频繁地使用于社交网络、身份证、学历验证等方面，这一节我们将从一个比较具体的方面——身份证讲起。

当区块链遇见身份证，会产生怎样的化学反应？如果区块链世界有身份证，又会长什么样？下面，我们就来研究一个神奇的名词——“分布式智能身份认证系统”，也就是区块链世界的“身份证”。

身份证是一件神奇的东西，平时不显眼，离了它却又寸步难行。身份证是用于证明持有人身份的证件，我们住酒店、买车票处处都会用到它，一旦丢失、忘带、被盗用，简直就是一场灾难。

如果你还在担心身份证引发的各种问题，那么基于区块链技术的智能身份认证系统或许可以帮你消除困扰。属于你的区块链身份证会显示你的护照照片、在线头像，姓名下方有一个不可更改的密钥创建日期以及密钥标识，这张身份证上还分布着签名栏、专属二维码、交易编号以及哈希算法证明。



图4-10 身份证引发的问题

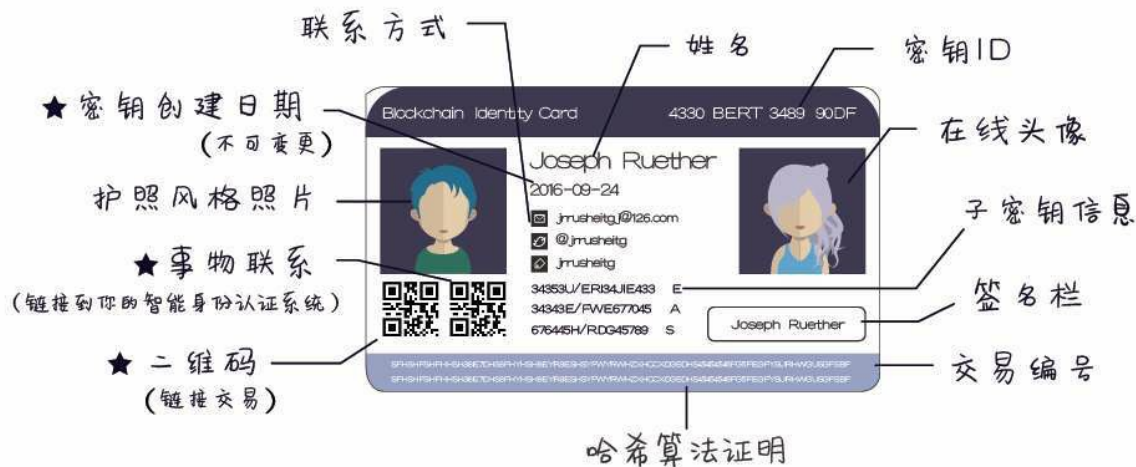


图4-11 区块链身份证

下面详细介绍创建并使用区块链身份证的步骤，大体分为三步：

1. 取一个独特的名字

这样其他人就能找到你的区块链ID，只要你好好保存你的密码，那么没有人可以夺走你的名字。

2. 创建并确认你的个人档案

把你的区块链身份证和社会网络档案连接起来，证明这是你本人的区块链身份证并确认你的个人信息。

3. 开始使用你的区块链身份证

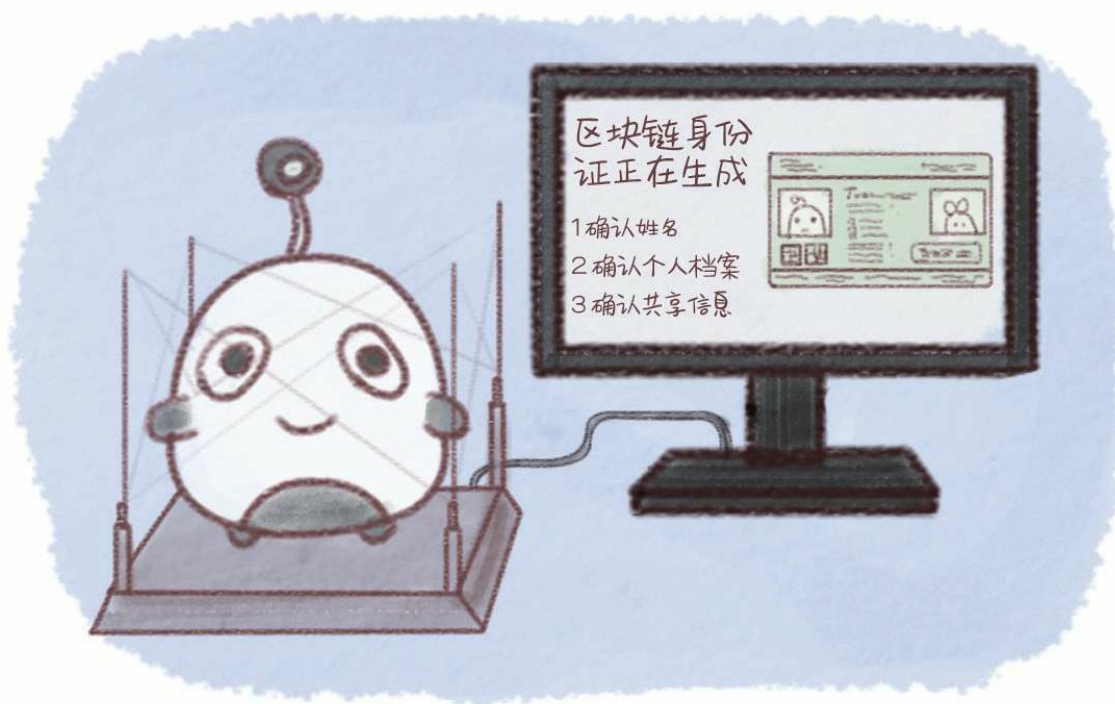


图4-12 生成区块链身份证

把你的区块链身份证共享在你的网页、社交网络档案以及名片上，这样人们就可以很容易地在网上找到你了。

区块链身份证有两个优势：安全、便捷地解决信息丢失问题；永远不会丢失、永远不会被篡改。



图4-13 区块链身份证优势

如果每个人都有一个区块链身份证，就相当于每个人都有一份完整、独特、记录了一生中每一笔交易的永久记录。在未来，区块链身份证可能不会一下子就将所有的社交等信息全部连接到一起，却很可能取代身份证、指纹、护照等身份识别工具。

当然，如果真的有一天，你拥有了区块链身份证，一定要妥善保管密钥，因为无论进行任何操作，都需要提供密钥来进入个人账户，而唯一的密钥只有你自己知道，所以一定要记得备份。

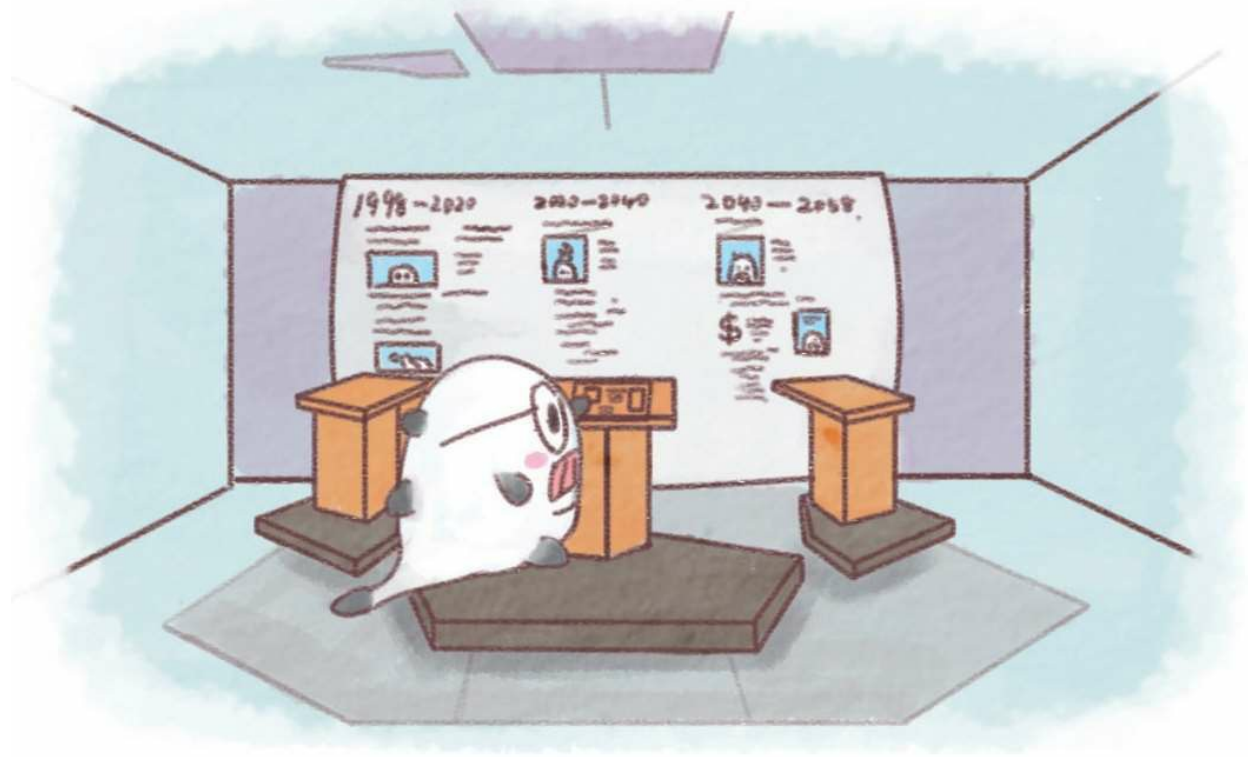


图4-14 记录一生的区块链身份证

到那时，甚至虹膜识别等生物识别技术也许就根本用不到了，毕竟，黑客攻击一个系统首先要做的就是侵入，然后才能进行篡改。但是在区块链系统中，登录动作也是一笔“交易行为”。如果有人想要以冒名顶替的方式登录已经采用区块链技术的系统，就等于要在千亿台电脑上登录资料链，几乎没有成功的可能性。如果真的到了那一天，指纹或者瞳孔扫描之类的技术，都会变得不是那么必要了。

案例一：霍伯顿软件工程学院

2015年10月，美国旧金山的霍伯顿软件工程学院宣布将利用区块链记录学生的学业完成情况，成为世界上第一个利用区块链认证学历证书的学校。

霍伯顿软件工程学院的联合创始人西尔万·卡拉什（Sylvain

Kalache) 称, 学校理解招聘公司在辨别学历真伪时面临的困难, 所以他们采用了区块链技术来认证学生的学位证。

卡拉什说: “对于雇主来说, 他们不需要花很多时间打电话去大学或者找第三方机构确认求职者的学历。”同时, 区块链还能帮助学校节省很多的人力和财力, 省去了建立数据库的麻烦。卡拉什还说: “我们的学生非常乐意看到他们的学位证能够得到认证, 他们同时也看到了这项技术的发展潜力。现在已经有很多公司投资开发区块链, 学生们非常骄傲我们学校能够成为第一个这么做的。”^[3]

案例二: 加拿大身份认证和鉴定服务公司 **SecureKey**

加拿大身份认证和鉴定服务公司SecureKey和加拿大数字身份验证委员会获得了美国国土安全局下属研究中心的资助, 将共同开发区块链数字身份网络。

SecureKey正在开发一种被称为“三盲”(triple blind)的保密程序。安装这个程序后, 如果某个人输入账号密码登录银行系统, 银行方面是看不到这些数据的走向的, 数据的接收方也不知道这些数据来自哪个银行或者哪个账户。同样, SecureKey对整个过程也是“失明”的。这就是所谓的“三盲”。

在采访中, SecureKey首席身份官安德烈·博伊森 (Andre Boysen) 说: “当今世界, 每个公司都各行其是, 数字身份系统搭建和运行的实现不可能靠单一个公司做到, 要实现用户身份数字化可能需要一个城市的人口那么多的人力投入。”

在当今这个技术飞速发展的世界, 人们必须要找到值得信任的技术验证个人身份, 防止身份盗窃问题的发生。SecureKey和加拿大数字身

份验证委员会正在为创造这样的技术而努力。[\[4\]](#)

区块链+能源

每当我们谈到能源领域的商业模式，区块链这一名词便不断被提及。风口之下，区块链在能源领域充满想象空间，引领着“互联网+”智慧能源的发展趋势与潮流。这一节我们将摘取《区块链在能源互联网应用的前景展望》一文中的部分观点，同时加以简要说明。概括来说，区块链在能源领域的应用主要有三个方面：电力、生态系统和能源智能化调控。

电力

区块链的重要特征之一就是数据的不可篡改性，而区块链在电力领域的应用就和区块链的这一特点密不可分。区块链技术的使用使每一度电的“前世今生”都会被记录在区块链网络上：某度电于某年某月产生于某核电站，经过某条线路输送到了我的家里，我在使用了几个小时的灯泡后这度电消耗光了。

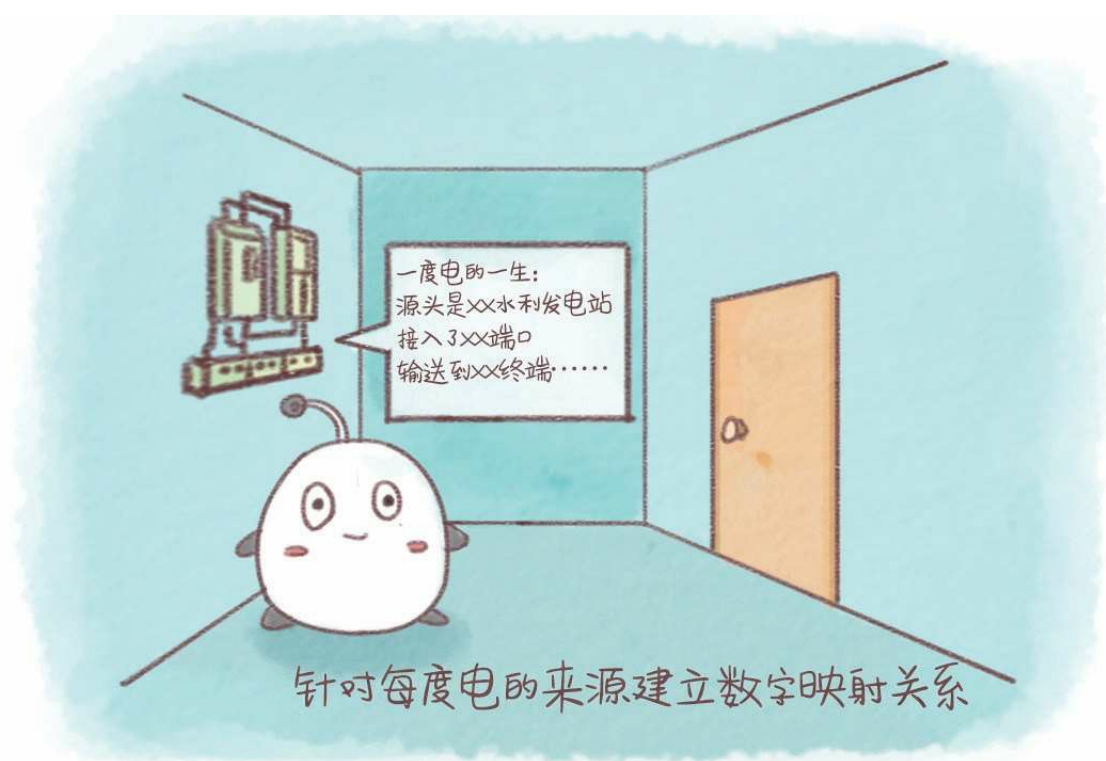


图4-15 区块链+电力

未来，区块链+电力可能会有以下几种发展方向：

1. 让每一度电都有迹可循，从根源上杜绝偷电漏电现象的发生。当一切行为都被记录在一个不可修改的账本中时，无中生有或是突然消失都会作为异常情况被处理。

2. 与邻居交易剩余的电。我们现在的电力系统其实已经有一点智能化的影子了，购电和断电都可以经由一个智能化的电表来完成。而去中心化的区块链技术的使用甚至可以让你和隔壁的邻居交易剩余的电。未来我们可以针对每一度电建立一个数字映射关系，比如你在家装了个太阳能发电器，每天能产生1度电，但你每天只能使用0.5度电，剩余的0.5度电就会归集到总网络中，隔壁的邻居想要用电的时候就可以直接选择与你交易。区块链让分布式的能源共享成为可能。

生态系统

区块链、物联网、大数据三者的结合可以打造出一个能源生态体系中的“乌托邦”。举个简单的例子，假设未来的某一天我们应用这三种技术建立起了一个能源生态系统，然后把设备供应商、专业运维服务商、使用设备的业主以及负责金钱流通和报价汇总的金融系统打包扔进这个系统做测试。接入这个系统的每一方都能得到一个此系统的查询密码，使用这个密码可以查询加密后的任何人接入系统后的任何动作，这样一来，这个系统中的四方或者说所有参与者就将形成一种交互监督、交互信任的关系。系统可以根据大数据分析直接计算出最适合业主的方案，并通过智能合约经由金融机构自主完成购买或者维修行为。

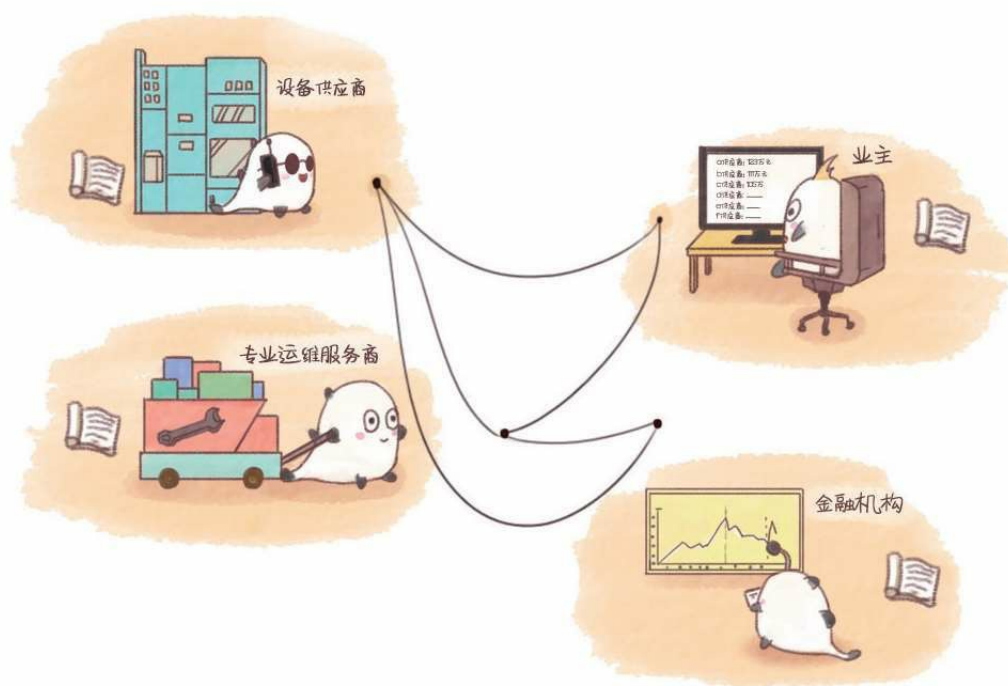


图4-16 交互可信的生态系统

能源智能化调控

未来，通过区块链技术，可以实现能源智能化调控，智能设备与互联网信息可以经由区块链连接在一起。想象一下，某市区的摄像头捕捉到郊区某一输电设备突然异常断电，与其他相关节点反馈的信息——比如报警器的鸣响或是某一区域灯光突然熄灭等对比并确认真实后，信息直接传递给维修总部，总部设备会根据智能合约的规则设定自动派出相应维修设备去往现场维修。智能化调控的时代会让我们的生活更加方便，更加安心。

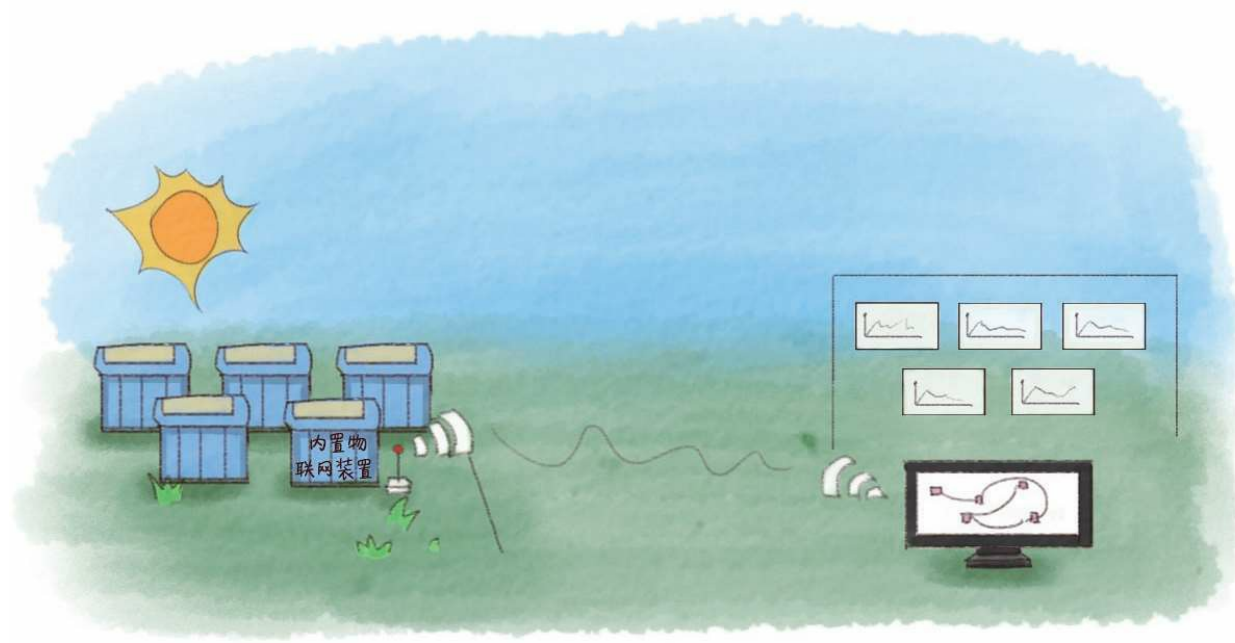


图4-17 能源智能化调控

案例一：能源传输项目**TransActive Grid**

纽约的区块链创业公司LO3与科技巨头西门子联手发展TransActive Grid项目，这是一个基于以太坊的能源传输项目。参与该项目的客户能够把剩余的电力卖给其他人。此前，LO3公司获得了美国专利商标局颁发的去中心化能量传输专利。

西门子能源管理部CEO拉尔夫·克里斯蒂安（Ralf Christian）

说：“我们相信，我们的微电网控制和自动化解决方案再加上合作伙伴LO3公司的区块链技术，将为我们公用事业领域的客户提供更多的附加价值。”

两家公司共同表示它们将在纽约和世界其他地区测试由区块链供电的微型电网，希望在未来能将区块链微型电网扩展到世界各地。[\[5\]](#)

案例二：能源区块链实验室

2016年5月15日下午，全球首个能源区块链实验室正式成立。能源区块链实验室由4位创始合伙人创办。这家实验室主要从事的工作是自主研发区块链平台，为能源金融产品的开发、审核、登记、交易提供全流程的协作工具。

实验室创始人之一、信达证券能源互联网首席研究员曹寅在接受钛媒体的采访时说：“未来的储能，更可能是基于分享经济的储能。储能的利用率单体就是单个企业购买的储能的利用率，它其实是非常低的，因为不可能一天24小时都把储能利用起来，但在区块链技术之下，储能可以像滴滴和优步的出租车一样，周边的用户都可以通过使用权的分享，调用某用户名下的储能设施，然后基于储能的收益付使用费给储能的所有者。”[\[6\]](#)



图4 - 18 能源区块链实验室的目标

区块链+政府^[7]

区块链具有去中心化、不可篡改、可信任、可追溯等特点，因此，区块链+政府也将引发一种新的时代变局。

基础信息保护

现今的政府信息系统采用的是怎样的模式呢？各下属部门的信息统一汇总至政府主管部门，主管部门有权调用各下属部门的信息。在这种模式下，黑客如果想要攻击政府的信息系统，只需要攻破中心路由就可以了，一旦黑客攻击成功，这一中心路由下储存的信息就很有可能全部泄漏、损坏丢失甚至被恶意篡改。

而将区块链技术应用于政府信息系统，系统的安全性将大幅提升。这样一来，所有的政府信息将分布式地储存在各个节点上，每个部门都有一个总账本，而且这个账本是经过哈希加密的，不可篡改、无法泄露。这样，就算黑客成功攻破了单一节点，政府信息不会丢失也不会影响整个系统的运行，因为其他节点都保存着一个同样完整的账本。而且在区块链系统中，仅仅修改某一节点上的数据是没有用的，它无法得到全网的认可。

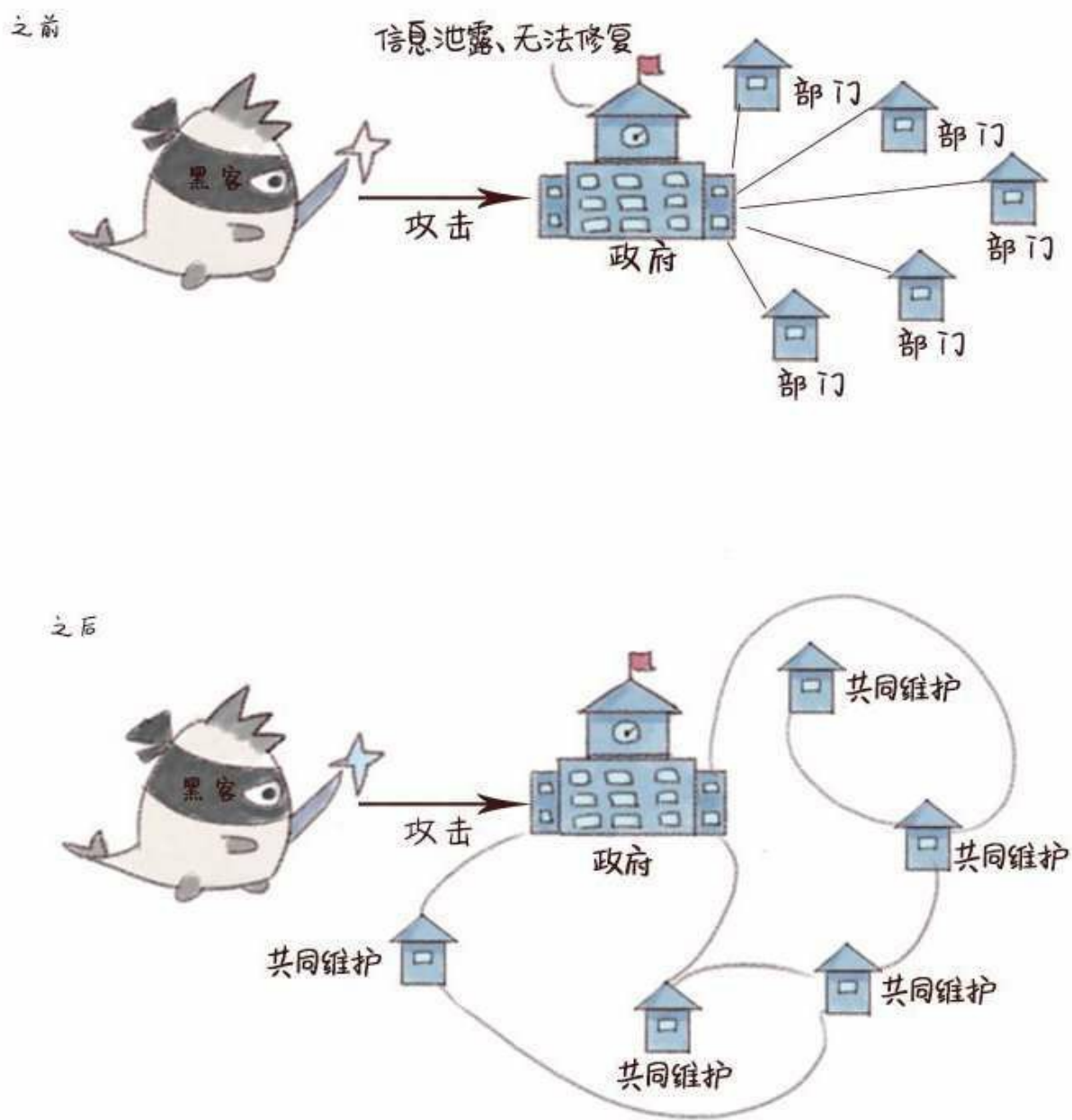


图4-19 区块链+基础信息保护

公民身份认定

想要证明你已经结婚了？请去民政局办理结婚证明。想要证明你妈

是你妈？不好意思，没有政府部门可以开具此种证明。可是某部门说如果没有这个证明我就无法办理接下来的手续。哦.....请前往其他相关部门咨询办理。

可以说，公民身份的认证是政府工作重要的组成部分，但是大量公民身份认证工作需要耗费巨大的人工成本。而应用区块链技术，可以使每个人一生的所有信息都储存在自己的“地址”上，随用随取。而且因为区块链信息的不可篡改性，人们也不用担心自己拿出的证明是无效的。基于区块链技术的、得到全民认同的公民信息认证系统可以有效地减少社会资源的浪费，而且可以尽可能地保证信息的真实性。

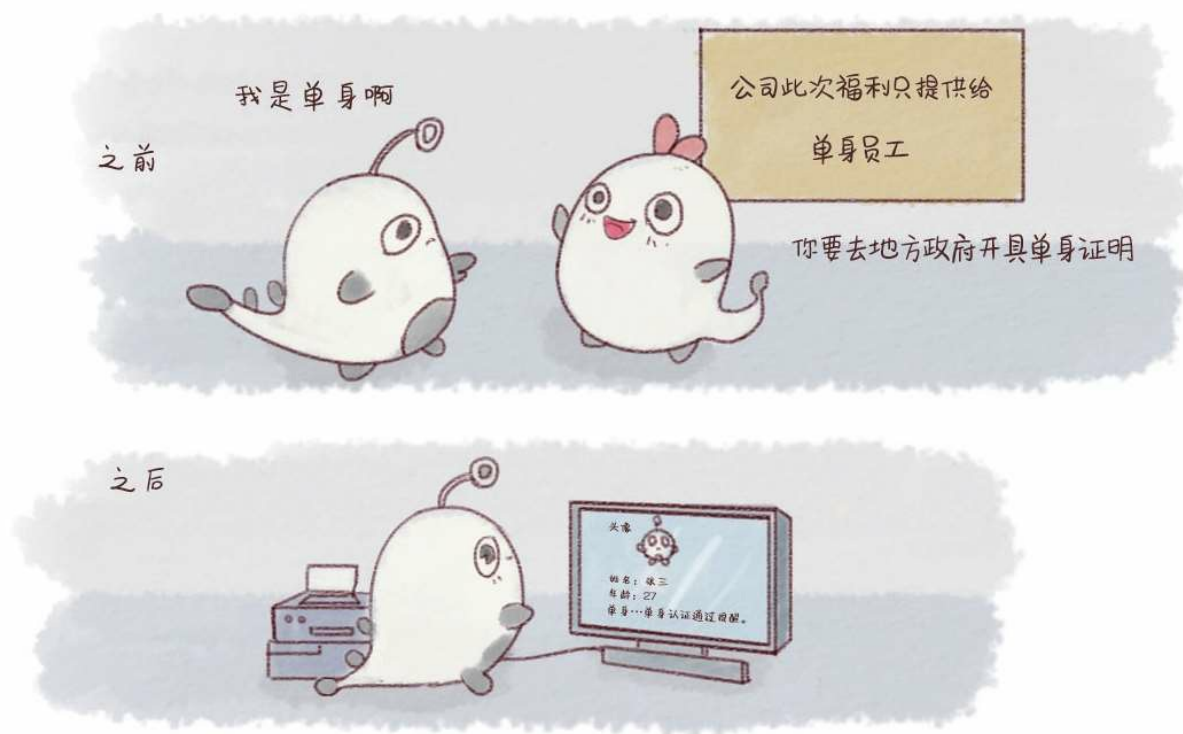


图4-20 区块链+身份认定

政务信息公开

如今，全世界的政府信息都不能说是完全透明的，我们只能看到法令的实施结果，却并不知道它的形成过程，所以一旦法令出现问题、需要追责的时候，站出来的往往都是“替罪羊”式的人物，这就会导致一种只能接受、无从监督的局面。

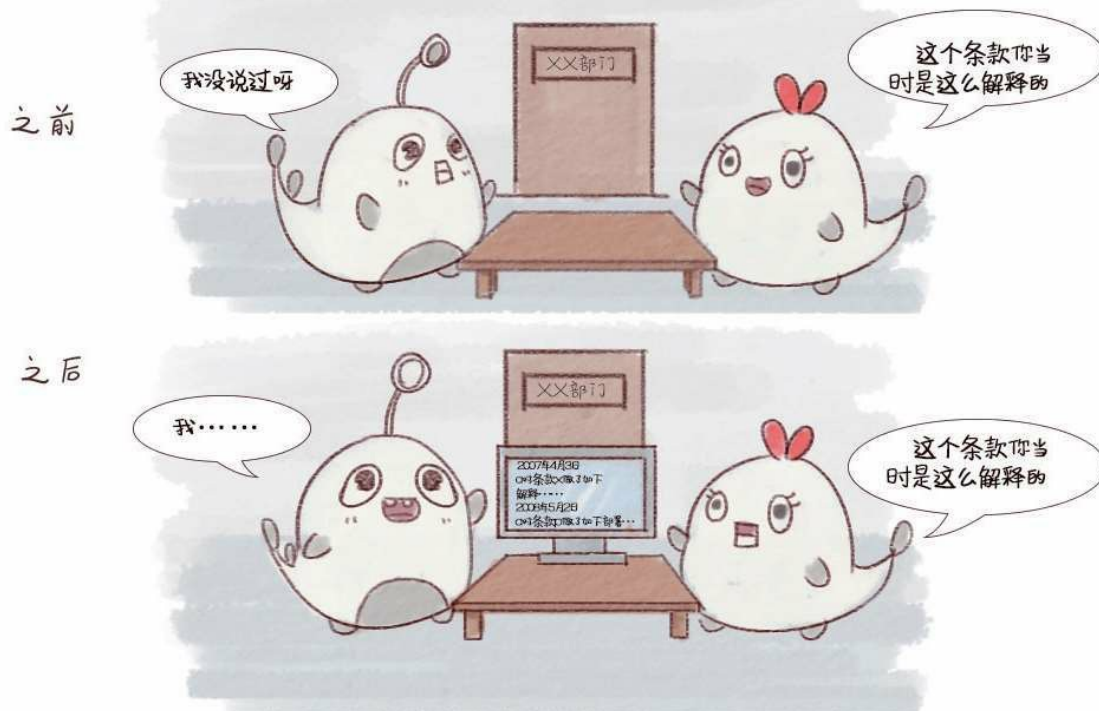


图4-21 区块链+政务信息公开

应用区块链技术，可以让政务工作更加透明，可以使政策的实施不会受到外力的干扰，而政策的可追溯性则会让决策参与人更加慎重。

政府税收监管



图4-22 区块链+政府税收监督

偷税漏税在全世界范围内都是一个重点问题，一部分企业或者个人通过伪造账目的方式达到避税的目的。应用区块链技术，可以从公司建立之初就建立一个分布式账本数据库，公司建立和运营过程中发生的每一笔资金流动都会在账本上体现，而且通过智能合约与其他公司的分布式账本数据库相互验证。每一笔账目都不可篡改且源头可追溯，这可以有效地杜绝偷税漏税的行为，而且一旦偷税漏税行为被查处，也会被永远记录在区块链上，无法抹去。

项目公开招标

在政府项目的招标中，一直存在亲近者得的现象，一个项目在满足预算要求的前提下由谁来实施可能很大程度上取决于投标企业与政府关系的好坏。企业投标之后只能等待结果，很多时候都不知自己为何落

选，而且就算中标的不是自己，投标方案也有可能后续建设中被使用，这个时候企业只能用也许就是凑巧来安慰自己。应用区块链技术，可以使所有投标信息透明化，有权限的人才可以调取相关记录，这可以从一定程度上遏制腐败的滋生。如果腐败记录永远保存在你的上司可以随时调看的“小本本”上，想必也就没有那么多明目张胆地腐败了吧。

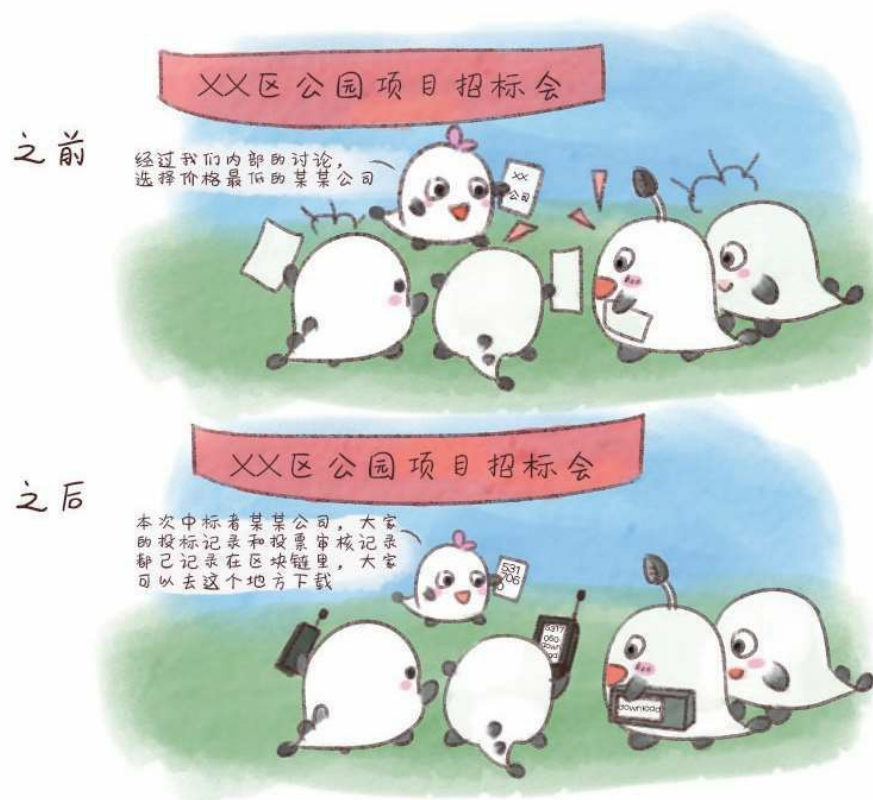


图4-23 区块链+项目公开招标

救助资金监管

很多人都愿意参加慈善事业，但是我们很难建立信任，慈善机构屡次爆出的腐败事件、公款挪用事件、作秀事件让我们对公益组织的信任度越来越低。而有时我们不适当的爱心也会成为社会的负担，比如我们把旧衣服按照网上搜到的地址捐赠到某个救济服务站，但其实这家服务

站的旧衣服已经多的成灾，而有的服务站却连一件都没有。

之前



之后

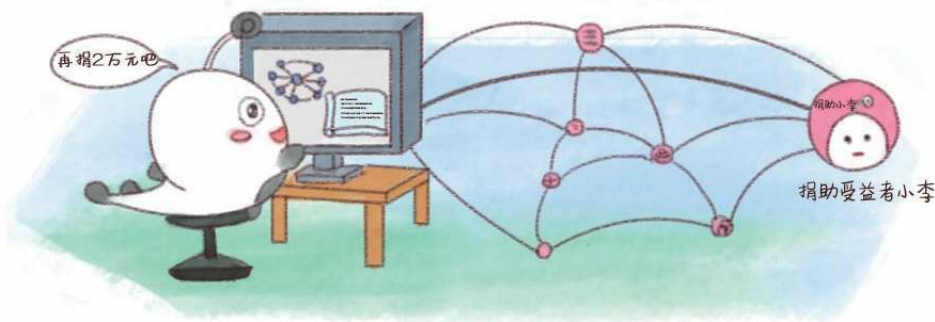


图4 - 24区块链+救助资金监管

使用区块链技术，可以实时监控个人捐款的流向，比如你于去年儿童节向某慈善机构捐赠了1元钱，区块链上的记录显示，这1元钱经过多次辗转最终变成了某留守儿童中心水果盘里的几粒葡萄。透明可查的捐赠让我们的爱心不会付之东流。

彩票网络发行

网络彩票在盛行一段时间后被紧急叫停，根本原因在于存在一些造假的商家。具体造假流程是这样的：你在网络上购买彩票后，商家并没有真正去到福利彩票中心购买一张真实的彩票，而是摇身一变，成了一家小型的博彩中心，如果你中了2 000元，那么平台会直接从自己的账户中划拨2 000元给你；如果你没中奖，那么你的2元钱就归商家所有。通过这种方式，最终结算下来，不法平台还是挣钱的。但是存在这样一

个问题——一旦你中了2亿元呢，平台给不起，那就只能跑路了。

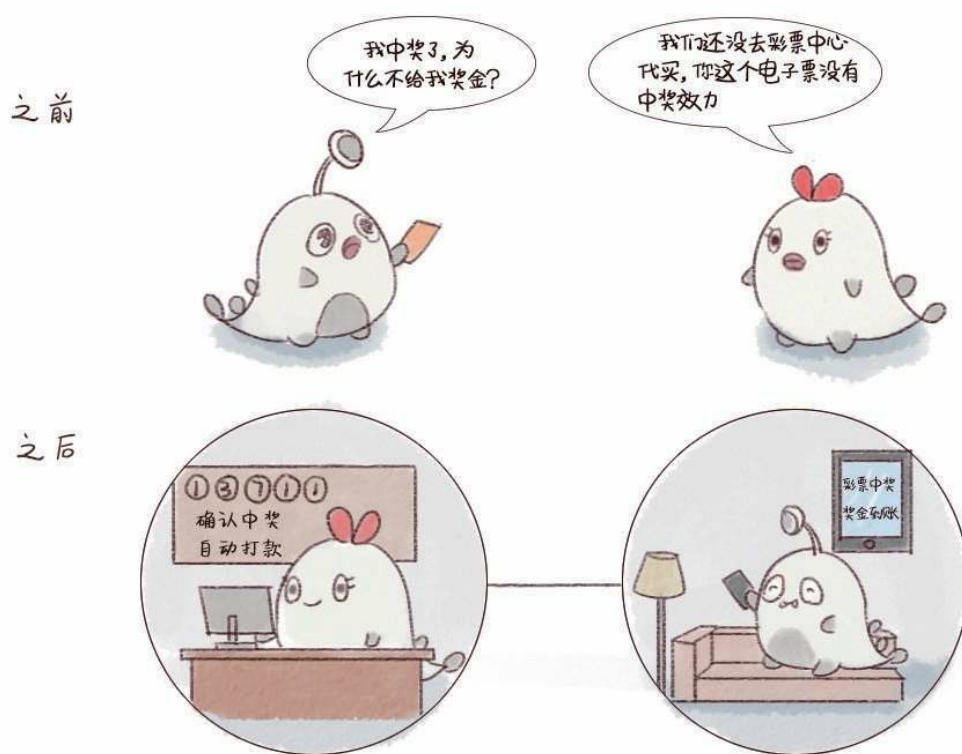


图4-25 区块链+彩票网络发行

区块链技术搭配智能合约可以解决网络彩票发行存在的造假问题。每一次购买行为都公开可查，彩票中奖后，智能合约会将钱自动打到彩票购买者的账户中。

案例一：爱沙尼亚政府的“电子居民”计划

爱沙尼亚政府计划面向全世界发行数字身份证，以帮助人们在爱沙尼亚管辖范围内开展网上交易。获得爱沙尼亚“电子居民证”的外籍人士并不会自动获得在爱沙尼亚境内的实际居住权，但是他们可以在网上与爱沙尼亚人进行贸易往来。

“电子居民”可以对证书、合同等文件在线设置数字签名、验证和加密。一旦开户完成后，爱沙尼亚的“电子居民”就可以通过电子银行遥控银行账户向世界任何国家转账汇款。[\[8\]](#)

案例二：Follow My Vote投票系统

Follow My Vote公司致力于利用区块链技术打造一种开源的、可审计的、安全高效的端对端投票系统，防止投票过程中出现安全漏洞。

投票者无须在投票站前排队等待投票，只需要在家中使用网络摄像头和政府颁发的身份证件就能完成投票。区块链的可审核特性，保证了所有选民都能看到实时投票情况；区块链的分布式账本能够保证每张选票都是匿名且不可篡改的。此外，每位选民都能通过他们的私钥和选民身份证随时更改他们自己的选票。

Follow My Vote公司的联合创始人兼首席技术官内森·乌尔（Nathan Hourt）认为纸质投票系统并不实用，撇开票数庞大很难统计的问题不说，统计票数完全依靠人工，这就要求票数统计员精确且诚实地进行统计。“这样一来，你就没办法查出安全漏洞到底在哪，也不能保证所有的纸质选票都能得到很好的保存，也不知道是不是有多余的选票混进来，或者有没有一部分选票被篡改。这种方式实际上将风险扩大了，票数越多，越容易发生骗选和腐败。”[\[9\]](#)

区块链+医疗

区块链技术的诞生，使得全员人口数据库和健康信息交易所变得落伍。区块链技术可以提升数据的安全性，节省显性及隐性成本。如果新的医疗记录方式成为现实，2016年年初的劣质儿童疫苗悲剧就再也不会发生了。

中投顾问在其发布的《2016—2020年区块链技术深度调研及投资前景预测报告》中把区块链技术在医疗领域的应用分为了以下几个方面：电子健康病例、“DNA钱包”、药品防伪和蛋白质折叠。[\[10\]](#)

电子健康病例

我们在不同医院就诊时会被发放不同医院的病历，而各个病历之间是不相通的，如果患者不主动提供或者想不起来提供他在其他医院的过往病历，医院是无法获得的，这会在一定程度上阻碍诊疗的进行。而使用区块链技术，每个人的医疗数据都会保存在一个专属于自己的电子病历上。

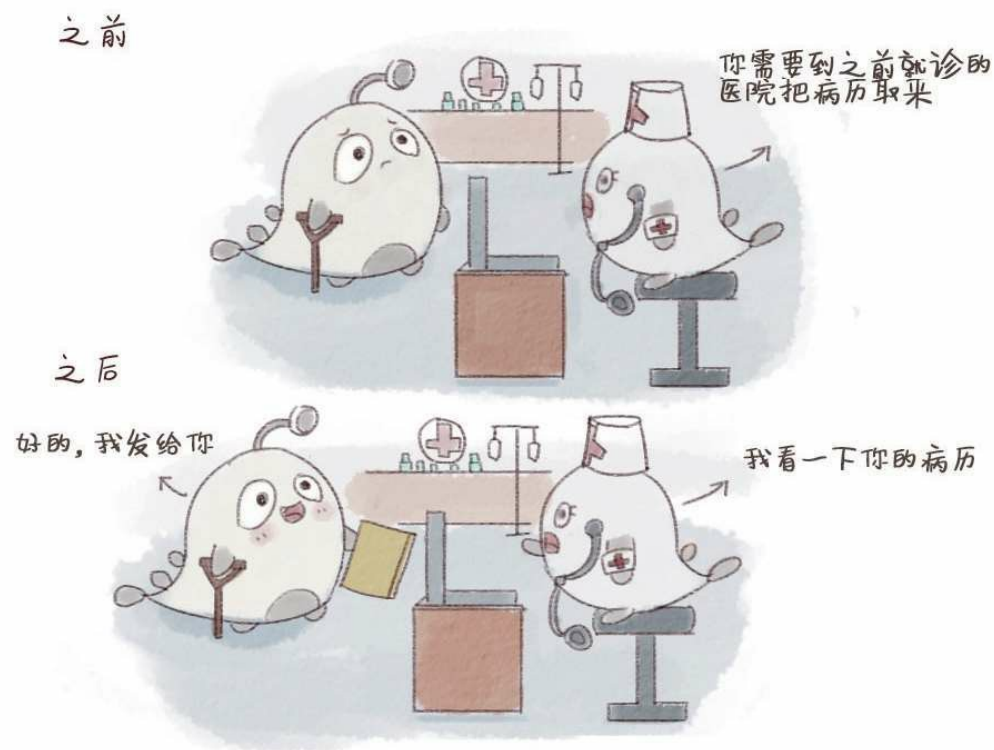


图4-26 区块链+电子健康病例

“DNA钱包”

基因和医疗数据可以通过区块链技术安全存储并通过私人密钥获得，这将形成一个“DNA钱包”。医药企业在进行药物研发时可以根据授权级别自动调取全网的相关数据，这对药物研发有很大的帮助作用。

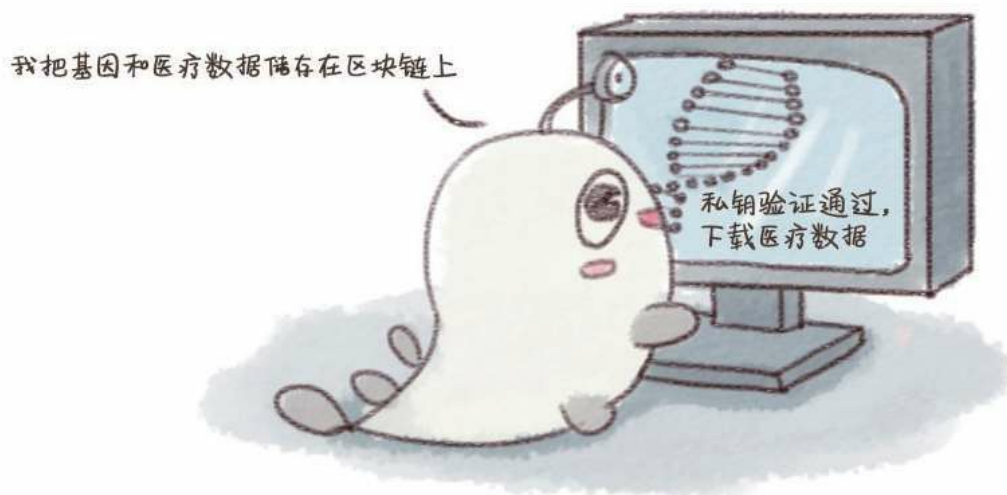


图4 - 27 区块链+ “DNA钱包”

药品防伪

区块链技术在药品防伪领域的应用与前面提到的身份认证极为相似，都是利用区块链可追溯的特点，赋予药品原料与成品唯一的编码，使造假者无法钻空子，而生产假药唯一的结局就是查无此数据。

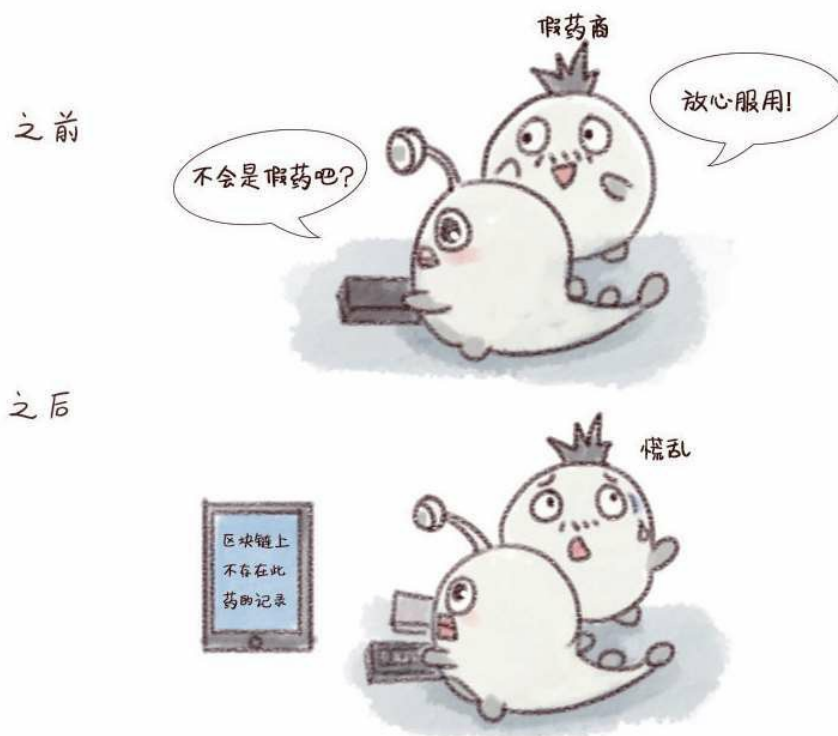


图4-28 区块链+药品防伪

蛋白质折叠

蛋白质折叠的过程模拟起来十分费力，斯坦福大学先前依赖非常昂贵的超级计算机来模拟蛋白质折叠的过程，但这种方式的缺点很明显：花费巨大并且存在单点故障。

而利用区块链技术可以建立一个分布式网络协助折叠蛋白质。节点网络中的每个节点在进行运算时都可以调用全网的算力，当一万台计算机合力帮你计算一个数据的时候，也就无须购买昂贵的超级主机了。

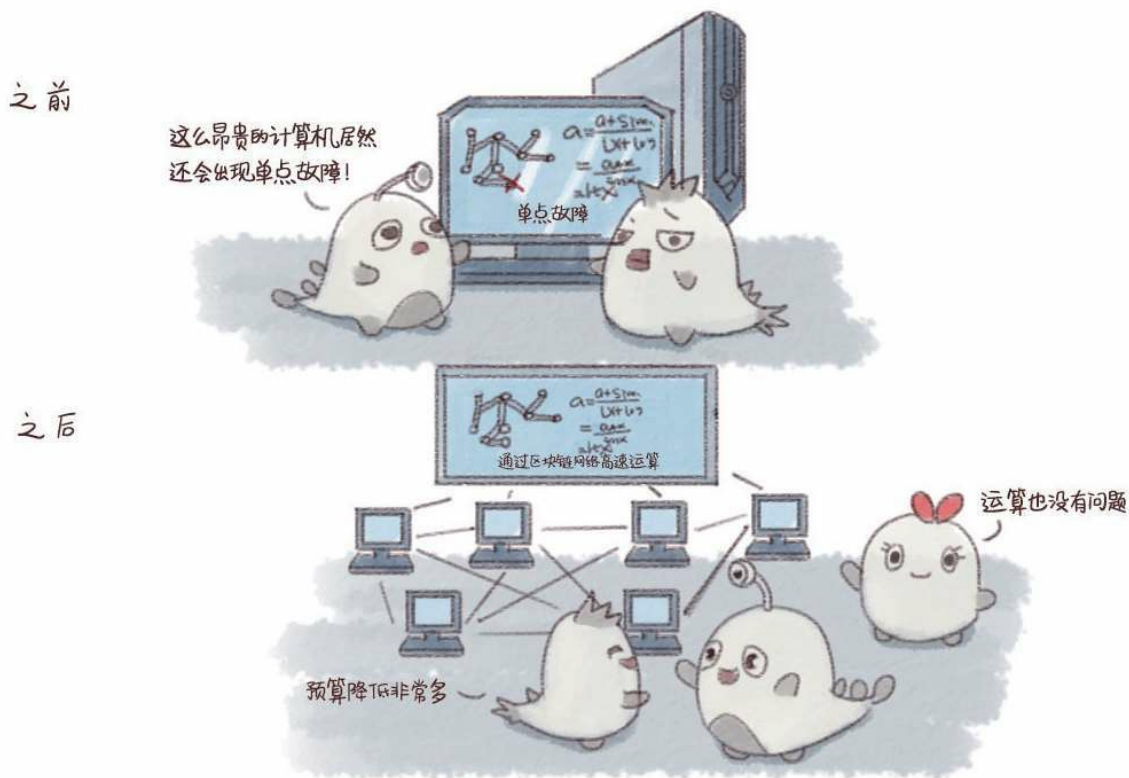


图4-29 区块链+蛋白质折叠

案例一：Guardtime与爱沙尼亚电子卫生基金会

数据安全初创公司Guardtime宣布与爱沙尼亚电子卫生基金会确立合作伙伴关系，利用区块链技术为100多万名患者的医疗记录提供安全的信息保障服务。

基金会将采用Guardtime公司的无钥匙签名基础设施，将医疗信息整合到基金会的Oracle数据引擎中，为患者提供实时可见的信息查询服务。患者的医疗记录也将被记录在区块链系统中。Guardtime公司的发言人在接受采访时表示：“我们在保护敏感信息时，遇到的最大威胁来自黑客、恶意软件和系统问题，数据可能因此被篡改、删除，或者出现更新错误等情况。但是有了区块链的话，情况就大不相同了，我们可以保证数据的完整性，所有的改动都会被记录下来。”

电子卫生基金会的负责人认为Guardtime公司的技术能够帮助他们对健康记录进行实时观测：“它让我们能够对任何突发事件做出快速反应，防止出现大规模的损失。”[\[11\]](#)

案例二：Brontech的医疗服务平台

澳大利亚悉尼的初创公司Brontech正使用区块链技术搭建服务平台，提高医疗保健系统的可信度和安全性。该健康平台被称为Cyph MD，采用区块链技术实现医疗保健中的数据共享。Cyph MD利用非对称加密技术，也就是使用私钥和公钥对数据进行加密和解密。非对称加密技术与分级证书系统的结合，使得每家医院都可以为本医院的医护人员设置“身份令牌”，方便医疗行业人员之间的沟通。

Brontech公司的创始人埃玛·波波萨（Emma Poposka）表示其公司正专注于身份识别模块的开发：“我们正在努力创建一种像有防弹服保护一样的安全数字身份，而且所有人都能使用这个数字身份，甚至是那些在当地不具有合法身份的人。我们正在利用区块链技术开发一个多功能的身份平台，可以应用于不同的领域，其中一个教育，另一个是医疗保健。”[\[12\]](#)

区块链+版权

版权热，区块链更热！经过《小时代》《致青春》《盗墓笔记》等一系列电影的狂轰滥炸，普通群众也知道版权这个概念了。我们都知道版权就是钱这个道理，换句话说，谁手上的版权多，谁的话语权就大。

重金之下，必有纷争。《夏洛特烦恼》被媒体爆出全片抄袭自一个美国老片，《芈月传》的作者和编剧都说版权是自己的，更别说随处可见的“一个版权供全球”的盗墓系列了。

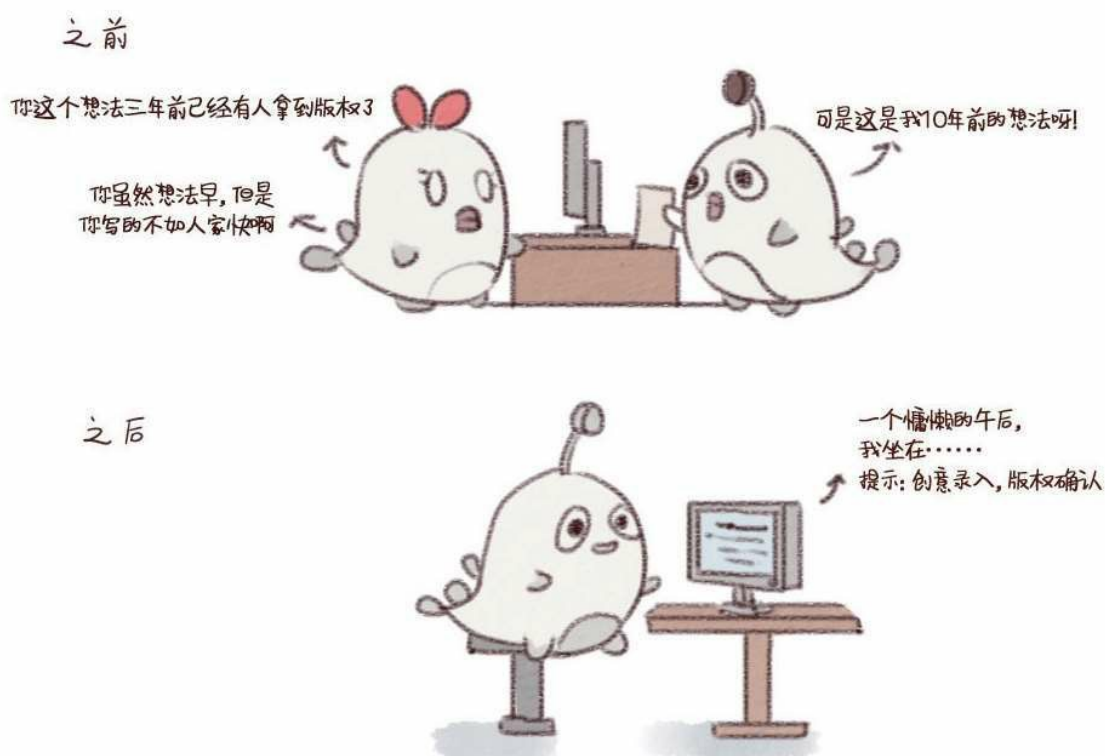


图4-30 区块链+版权

这些问题的根源，是版权的归属和保护问题，这是一个迫在眉睫的问题。之前很难解决，是因为维权成本太高，让原作者心力交瘁，如今

有了区块链，该出手的时候就要果断出手了。

我们来看看如何利用区块链技术解决版权问题。首先便是宣布所有权，加盖时间戳。

创作者可以将自己的原创作品及相关协议上传至区块链，随后，将会生成一个与文件对应的哈希值。在之后的交易中，可以将文件的加密哈希值插入其中，当这笔交易被区块链矿工打包到一个区块后，该区块的时间戳就成为该文件的时间戳。这张哈希值+时间戳的数字证书将在一定程度上解决存在证明和作品时效性的问题。

其次，所有权跟踪，全过程追溯。

在所有涉及版权使用和交易的环节，区块链都可以从头到尾记录下来，从而实现全过程追溯，而且整个过程是不可逆且不可篡改的。此外，区块链技术的应用还能在一定程度上解决无形资产确权和价值评估问题。

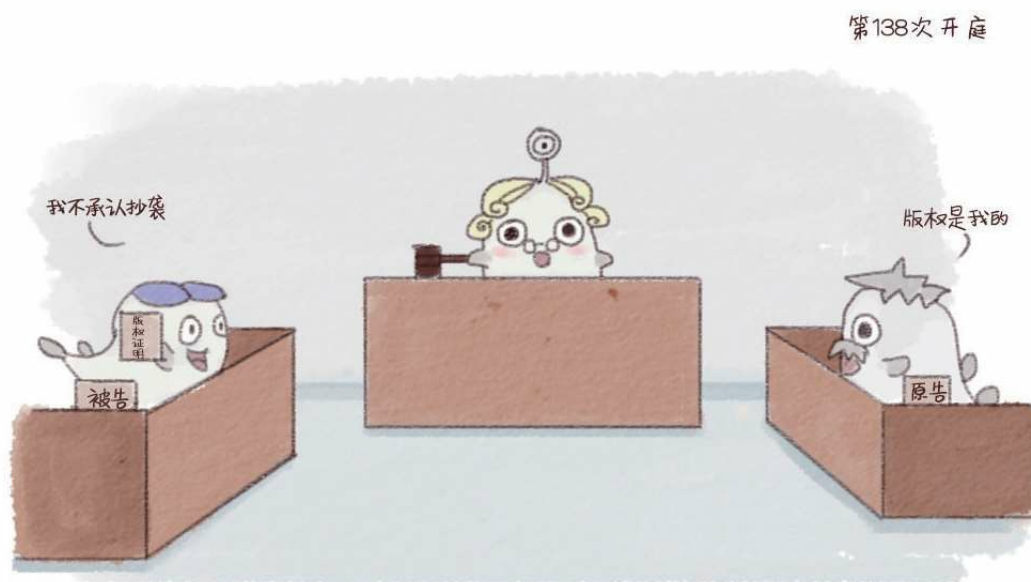


图4-31 版权难维护

国内的社交出版平台“赞赏”甚至提出“版权在作品的创作过程中就应该被确权”。也就是说将一个未成型的、只有几百字的创意开始到作品成型的全过程记录下来，并且让作品从创意阶段就有可能被确权进入交易环节。

“赞赏”期望通过智能合约规范所有作品权利的行使与追溯，同时在作品创作过程中即引入版权服务商进行交易。

这可以被称作区块链的版权一条龙服务，从源头到产品，一旦确权便不可修改。我们可以设想一下，如果区块链版权证明大规模推广，那些抄袭者们也不会像如今这样猖狂。

利用区块链技术解决版权维护问题，看上去是一件很美的事情，但实际上它面临着三大挑战：

1. 区块链技术的商业化应用和大众化普及，就像如今流行的VR（虚拟现实），虽然概念已经脍炙人口，但普及率依然很低。



图4-32 区块链技术在版权应用中面临的三大挑战

2. 与区块链技术相关的法律从提案到制定再到修订要走的路，并不比区块链概念普及的里程短，这就导致目前还没有一起成功利用区块链维权的版权大事件。没有法律依据，创作者们持有的区块链凭证便只是一个安心证明而已。

3. 哈希值的生成花费巨大。它是根据文件大小、时间、类型、创作者等计算出来的，单一因素的细微改变都可能引起最终结果的巨变，谁也无法预料下一个哈希值是多少，也没有更改它的软件。这就增加了过程成本，如果没有巨头愿意牵头做这样一个系统，推动区块链为版权保驾护航就不知道还要多少年才能实现。

案例一：Babyghost与BitSE

在2016年的上海时装周上，独立时装品牌Babyghost与上海区块链服务公司BitSE共同展示了20套服装新品。所有展示的服装都内附BitSE公司生产的VeChain芯片，观众只需扫描芯片，就能收到一条信息，显示这套衣服的“前世今生”。BitSE公司表示，如果有顾客购买了这套衣服，穿了一段时间后想卖出的话，他的购买和穿着信息也会在芯片上留下记录，传给下一位买家。[\[13\]](#)

案例二：区块链与音乐

2015年10月，英国女歌手伊莫金·希普（Imogen Heap）将她的新歌《Tiny Human》发布在了以太坊的区块链上，用户只需将以太币存入其账户便可以获得MP3音乐文件的使用权限。这在保证用户能够获得版权授权的同时，也使希普及其团队能够及时且直接地获取收入。[\[14\]](#)

区块链+物联网

如果说10年前选择互联网是坐上了动车的话，现在选择区块链+物联网就是坐上了火箭。万物互联是未来的发展趋势，比如我们最常见的家居智能系统使我们可以用一部手机远程控制家中的所有电器。近年来，随着科技的飞速发展，物联网已经得到了加速进化。根据国际数据公司最新发表的一份统计报告，到2020年，全球物联网市场规模将增长至3万亿美元，而全球物联网设备将达到300亿台。



图4-33 简易的物联网

如今十分火热的区块链技术可以在物联网中的设备之间建立低成本连接，还能通过去中心化的共识机制提高系统的安全私密性。同时，区块链技术与智能合约的叠加能够把每个智能设备变成可以自我维护调节的网络节点，这些节点可以在事先规定好的基础上交换信息、核实身

份，同时与陌生人进行交易。

下面以电缆网络为例进行说明。现有的电缆网络普遍存在安全隐患和浪费现象，想象一下，智能化的电缆桥架会有多么安全、方便和实惠。一旦智能电缆桥架遭遇雷击，它可以及时生成事故报告，并通知维修队携带适合的工具前往指定地点进行维修。同时智能电缆桥架还可以将信号传输任务暂时分配给附近的电缆杆，毕竟它们属于同一个网络。这样一来电信公司就无须花费高昂的现场检修成本，而且可以尽快恢复通信。

在区块链+物联网的世界里，每根电缆桥架都是有身份的，没有身份就无法参与运行。用于身份认证的区块链是智能电缆网络的核心，工程师会为每个设备（电缆桥架）设定独特的线路，然后把这个线路和身份一同存储在分布式账本中。

分布式账本可以保证这些设备只有在收到费用后才能继续运行。如果发生损坏，智能电缆网络会迅速反应，自动寻找新的线路，防止大面积的通信中断。

这只是一些有关电缆桥架的设想，如果你展开想象力，就会发现，无论是最微小的传感器，还是巨大的机械设备，都可以连接到庞大的物联网中。

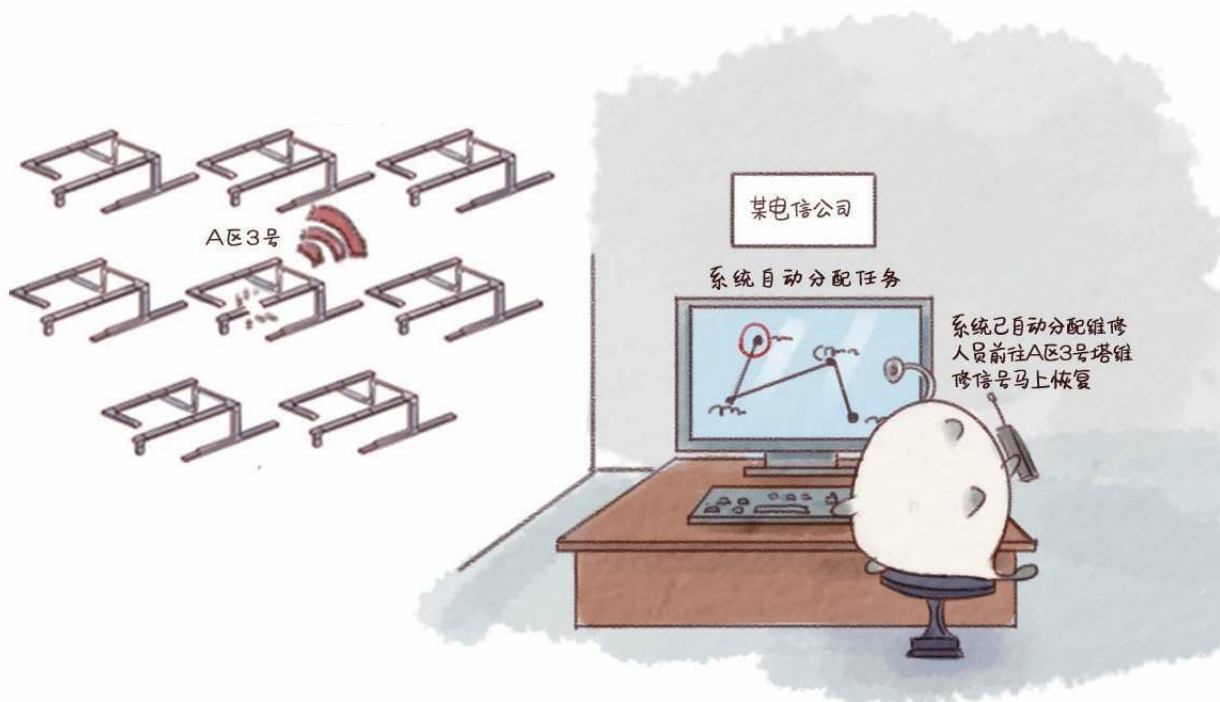


图4 - 34区块链+物联网

物联网的应用范围十分广泛，遍及智能交通、环境保护、政府工作、公共安全、智慧城市、智能家居、环境监测、工业监测、食品溯源等多个领域。物联网发展面临的最大挑战不是简单地建立一个去中心化的物联网，而是建立一个规模可以不断拓展的通用物联网，同时保证隐私、安全，使参与者无须建立信任便可进行交易。物联网中数以千亿计的参与者不都是值得信任的，有的甚至是恶意的，所以需要某种形式的验证和共识机制。

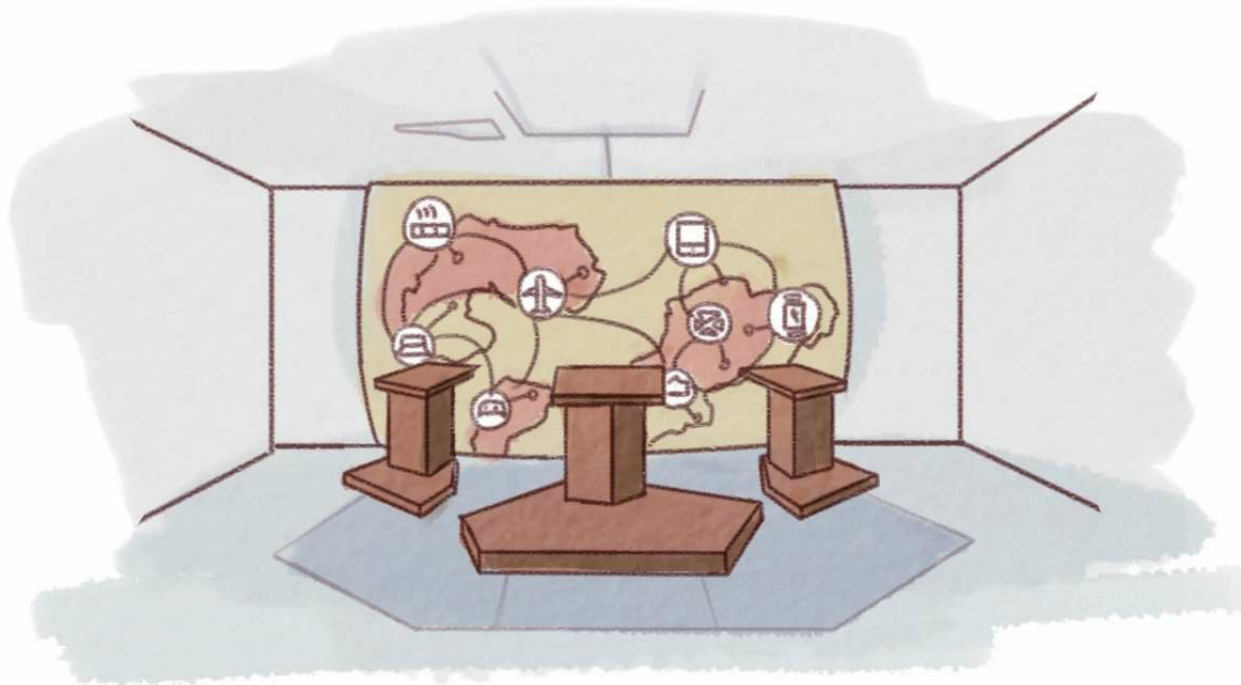


图4 - 35 区块链与万物互联

可以预见的是，在未来，这个星球上的几十亿人和几千亿部机器全都会连接到一个区块链网络之中，人与机器、机器与机器之间的交流对话、交易、支付将成为现实。人类正向着商品和服务几乎免费的时代加速迈进，而区块链+物联网的世界，就是去中心化与协同共享的世界。

案例一：Filament

近日，美国区块链创业公司Filament完成了500万美元的A轮融资，投资方分别为Bullpen Capital、威瑞森风投和三星风投。采用Filament公司基于区块链的堆栈，企业可以在不依赖中心化云和人工纸质办公的情况下，更加高效地管理采矿作业和水资源调动。

Filament公司的联合创始人兼首席执行官埃里克·杰宁斯（Eric Jennings）将Filament定义为一个去中心化的物联网软件堆栈，能够利用区块链技术在公共账本中记录设备的唯一身份。他说：“通过创建智能

设备目录，Filament将使物联网中的设备安全地沟通信息、执行智能合同和发送微交易。”

杰宁斯在接受媒体采访时表示：“几乎所有公司都有这样一种担忧——‘我的物联网战略是什么？’许多公司对它们本身所在的领域非常了解，但它们对于网状网络或区块链知道的很少，但是它们知道必须要与这些网络连接，提高效率，以免在行业发展中被踢出局。”[\[15\]](#)

案例二：IBM与三星

IBM（国际商用机器公司）宣布与三星合作开发ADEPT（去中心化的P2P自动遥测）系统，该系统使用比特币的底层技术构建分布式设备网络，即去中心化的物联网。IBM和三星选择了BitTorrent（文件共享）、Ethereum（智能合约）和TeleHash（P2P消息发送系统）三个协议支持ADEPT系统。

根据已公布的项目草案：“将区块链概念应用到物联网世界将创造出无限的可能性。一旦产品完成装配，制造商就可以将其注册到通用区块链上，标志着该产品生命线的开始。一旦产品被售出，经销商或者消费者就可以在区域区块链（如某个社区、某个城市或者某个省）上注册该产品。”

草案撰写者解释道：“我们向公众演示了如何使用ADEPT系统。一个普通的洗衣机可以成为半自主的智能设备，能够管理自身的消耗品供应，提供自助服务和进行自我维修，甚至还可以与其他家庭中和外部的对等设备进行沟通，自动优化运行环境。所有这一切都是在没有中央控制器编排或调解的情况下进行的。”[\[16\]](#)

区块链+农业

人与人之间的关系从互相信任开始，之后才会有接触交流及进一步的共同作业，最终促进人类共同的发展进步，而区块链完美诠释了这一关系。作为比特币的底层技术，区块链允许系统中多人参与记账过程，也就是说，每人都有一个完全相同的账本，但谁都不可以删除或修改账本内容，无论是机构还是个人。既然区块链的实用价值及透明度都较高，在我国这个农业大国，区块链能否与农业结合得相得益彰呢？

我国农业现状

1. 从农业生产经营形态来看，目前农业生产经营依然比较传统、粗放，靠天吃饭的局面没有根本改变；
2. 从资源可持续发展情况来看，中国农业在生产过程中产生大量资源和能源消耗，致使生态环境破坏严重，直接影响生态安全、人民健康；
3. 从信息化程度来看，中国农业信息化、现代化进程还处于起步阶段，需要相关人士引入更多的先进技术，提升农业智能化水平；
4. 从食品安全角度看，法律约束、监管力度不够，以及部分企业、个人一味追求利益最大化等，导致中国食品安全问题依然层出不穷，人们对食品安全机制缺乏足够的信任。[\[17\]](#)



图4-36 我国农业存在的问题

基于我国农业现状，可与区块链技术结合的方向有两个：商品化与农业保险

1. 商品化与区块链：消费流程全透明。

生产商可运用互联网身份标识技术，将生产出来的每件产品的信息全部记录在区块链中，在区块链中形成某一件商品的产出轨迹。

举例来说，假如小王自产了10斤非转基因小麦，于是他在区块链上添加一条初始记录：小王于某日生产了10斤小麦。接下来，小王把这10斤小麦卖给了去集市赶集的小刘，于是区块链上又增加了一条记录：小刘于某日收到了小王的10斤小麦。之后，小刘把小麦卖给了城里的面包房，区块链上新增记录：面包房于某日收到了小刘的10斤小麦。接着，面包房把小麦做成了面包。最终，当消费者购买面包时，只需在区块链

上查询相关信息，就可以追溯面包的整个生产过程，从而鉴定真伪。



图4-37 消费流程全透明

2. 农业保险与区块链：提升农业智能化。

将区块链技术与农业保险相结合，不仅可以有效减少骗保事件，还能大幅简化农业保险的办理流程，提升农业保险的赔付智能化。比如，一旦检测到农业灾害，区块链就会自动启动赔付流程，这样一来，不仅赔付效率显著提升，骗保问题也将迎刃而解。

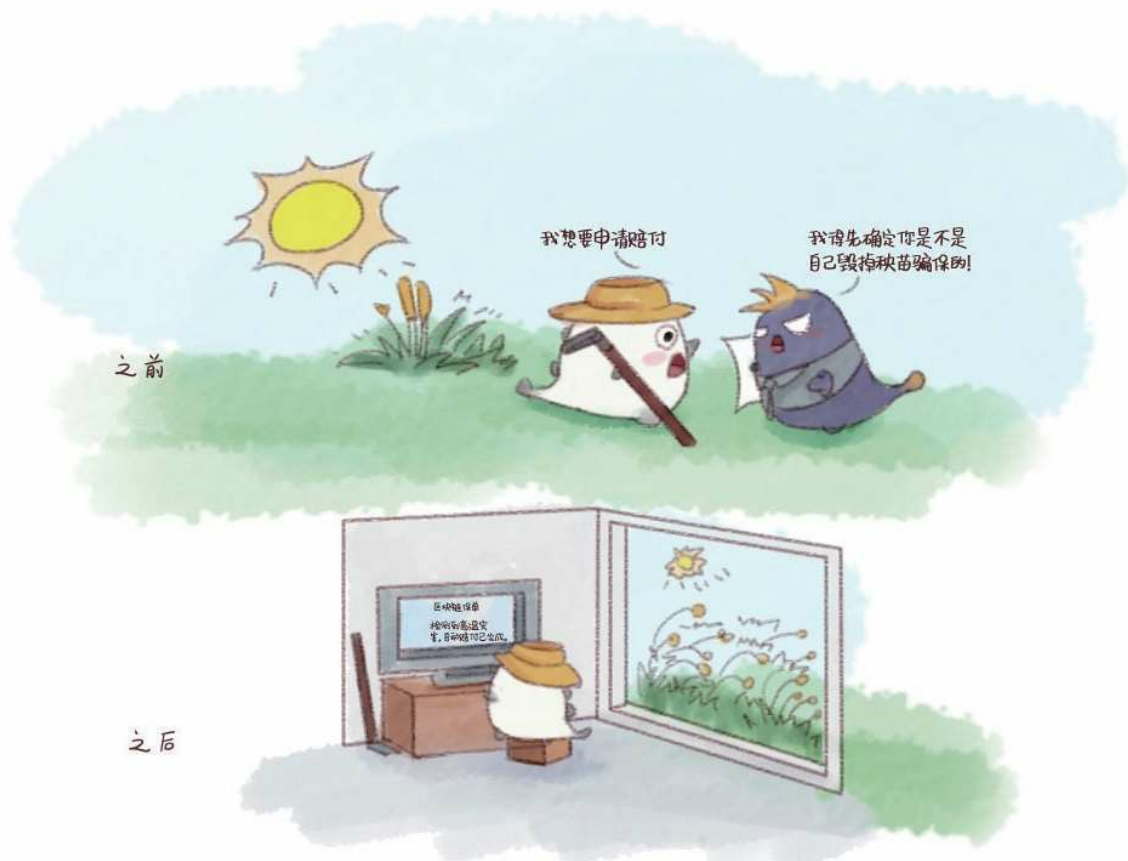


图4-38 提升农业智能化

案例一：沃尔玛的全球供应链

沃尔玛与IBM以及清华大学展开合作，在中国政府的协助下启动了两个独立推进的区块链试点项目，旨在提高供应链数据的准确性，保障食品安全。沃尔玛将区块链技术应用于全球供应链，成本将减少1万亿美元。此举不仅能够帮助中国更好地保障食品安全，更会为沃尔玛本身大幅度降低成本。

IBM全球供应链解决方案部门负责人解释道：“一旦这个试点项目投入运行，沃尔玛将从中国的猪肉市场获得更为丰厚的利润。”

该试点项目目前处于起步阶段，共安排了三个测试节点，包括IBM、沃尔玛和一家不愿意透露名称的供应商。负责人表示，等到后期

测试节点达到10个时，整个行业成本将减少“数十亿美元”。项目开展后，沃尔玛超市的每一件商品，都在区块链系统上完成了认证，都有一份透明且安全的商品记录。在分布式账本中记录的信息也能更好地帮助零售商管理不同店铺商品的上架日期。[\[18\]](#)

案例二：Filament的智能农场

根据Agfunder News（农业新闻网站）的报道，众多分布式账本农业解决方案正在兴起，包括创造出“智能农场”概念的Filament公司。在Filament公司的平台上，用户可以利用智能农场技术建造可靠的农场基础设施。所谓智能农场，就是一种可持续发展的农业生产模式，能够提高环境质量，整合科学技术与生物循环调节，通过农场运作创造经济价值。采用区块链技术的农场能够播报防篡改的气象数据、短信提醒、机械协议、GPS（全球定位系统）定位，并从其他相关平台上获取更准确的信息。

业内人士在解释区块链在推动农业经济发展中的潜力时指出：消费者对“干净”食品（包括有机食品）的需求急剧增加，但生产商和制造商通常很难保证从农场到餐桌这个生产流程中数据的准确性。在这个问题上，区块链可以提供很大帮助。此外，区块链技术在农业领域的实际应用还包括减少不公平定价、记录产品产地、减少进口农产品影响、发展本地化经济。在未来，区块链平台还可以帮助汇款到农村地区，提供农业金融解决方案。

区块链技术正向人们展示它改变全球市场和经济产业的潜力，农业领域将是其中之一。[\[19\]](#)

区块链+慈善

近年来，慈善捐款已变得越来越普遍，但该行业仍然存在着多年运作累积的很多问题。在某些特定的情况下，这些问题也阻碍了人们奉献爱心。

慈善援助基金会最近发布了一份题为“捐赠链——慈善和区块链”的报告，探讨区块链技术如何影响慈善机构筹集资金和运营的方式。该报告称，区块链技术可以改变人们对慈善事业的贡献方式，改变慈善机构使用捐款的方式。

根据这份长达20页的报告，2016年美国慈善机构的收入超过了2万亿美元，其中3730亿美元是慈善捐款。该份报告还分析了区块链技术在慈善领域的几种优势：

1. 降低交易成本

区块链上的交易是可以点对点完成的，你可以直接将钱捐赠给指定的人或机构，无须转手多家银行和机构，这将有效减少交易成本。

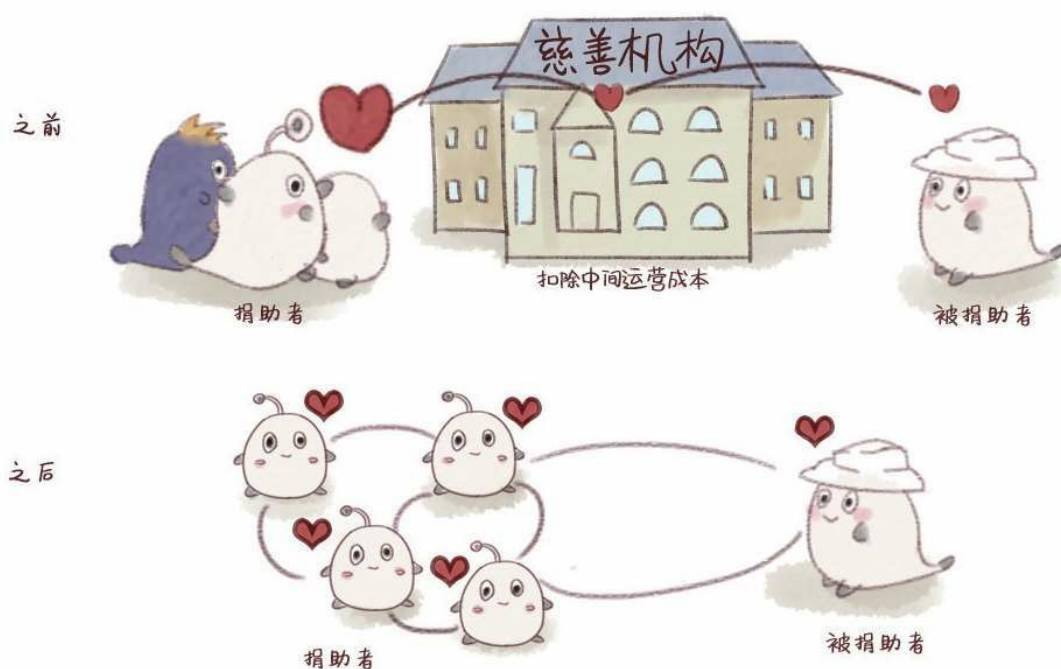


图4-39 降低交易成本

2. 增加透明度

区块链技术可以使捐赠的环节更加透明，每一次捐赠都会直接记录在分布式账本数据库中，记录公开透明可查询且不可篡改，当然，你也可以通过账本追溯捐款的去向。

3. 增强信任

区块链技术可以使人们快速建立信任关系，消除了捐助者对第三方的需求，这意味着2.0版的慈善机构和非营利性机构将不再依靠其他机构，如银行、律师和政府实体等。



图4 - 40 增加透明度

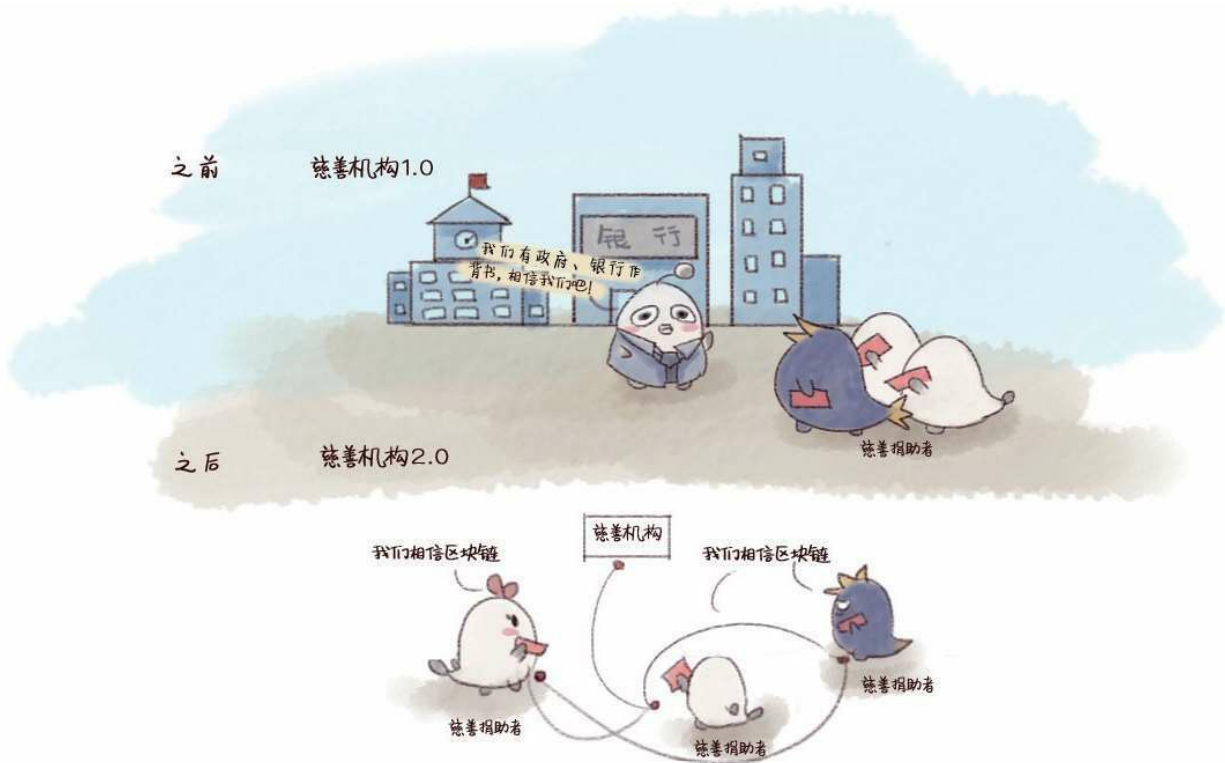


图 4 - 41 增强信任

案例：BitGive基金会

BitGive基金会自称是世界上第一个比特币非营利性组织。该组织与救助儿童会（Save The Children）和水资源项目（The Water Project）等非营利性组织建立了合作。

2016年3月，BitGive为肯尼亚西部的一所女子学校挖了一口水井，挖井的所有费用来自比特币社区捐赠的价值11 000美元的比特币。BitGive的负责人说：“该井现在为500名肯尼亚人提供饮用水，如果没有这口井，他们就无法获得干净的水。可以说，这口井的作用是非常巨大的。”[\[20\]](#)

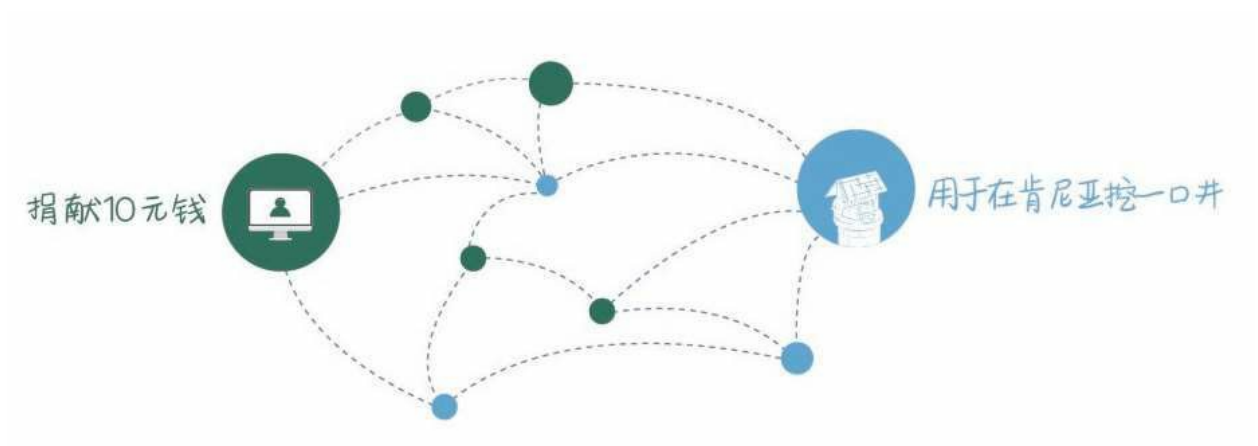


图4 - 42 区块链+慈善

区块链+其他

区块链的应用其实非常广泛，凡是与互联网有关的行业即可与之有所关联，包括有一些人们意想不到的领域。

补充一些区块链与之相融甚欢的特色领域，参考如下：

区块链+社交网络

Taringa!是拉美地区最大的内容平台，其发布了一个收入共享项目Taringa! Creadores，用户可以通过在其中发布内容赚取比特币。

区块链社交平台Steemit发布了测试版本，利用自己的区块链和加密货币对发布内容以及参与投票和讨论的人发放奖励。

Yours是另一个建立在比特币区块链上的分布式社交网络，预计在2016年年底发布。[\[21\]](#)

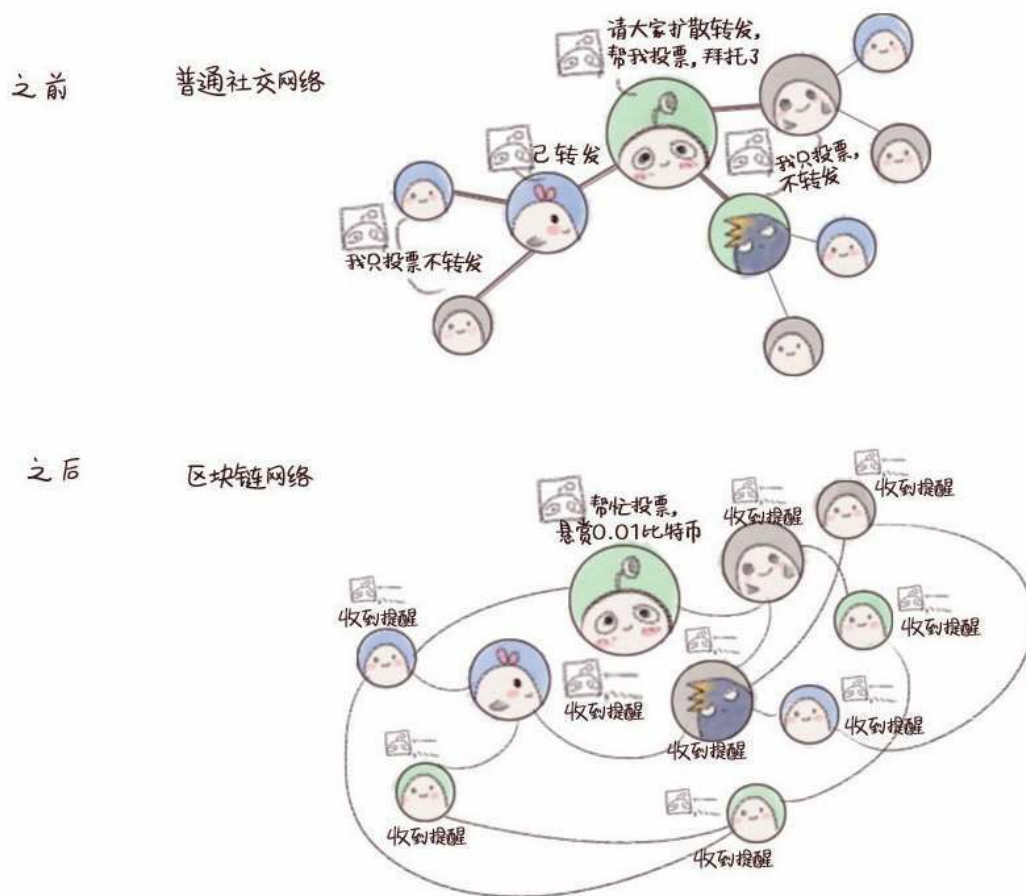


图4-43 区块链+社交网络

区块链+游戏

Takara是一款基于地理位置的游戏，玩家可以在该游戏设定的地图中寻找比特币和其他有价值的东西，包括优惠券、入场券、忠诚度积分、公司股票等。为了获取这些“宝藏”，玩家必须亲自跟随GPS到达指定地点。以上所有的奖励都会被记录在比特币区块链上。[\[22\]](#)

之前



之后



图4-44 区块链+游戏

区块链+火车票

当我们使用手机中的App（应用程序）购买车票时，信用卡公司会处理付费过程，并收取相应的手续费。但如果铁路公司采用区块链技术，便可以节省付给信用卡公司的费用，甚至还可以将整个购票系统搬到区块链上，实现购票透明化。



图4-45 区块链+火车票

区块链+电子邮件

如果能利用区块链发送电子邮件的话，邮件传输将更安全，甚至还可以解决垃圾邮件泛滥的问题，因为对于发送垃圾邮件的人而言，向这样的安全体系寄出几百万封垃圾邮件，恐怕是一种极不划算的行为。因为在区块链的体系中，用以交换的信息会经过验证、编码、执行，最后成为一笔记录，储存在一个不属于任何人的分散式网络中。另外，如果寄送邮件的成本极低，或许大家会愿意为了更高的安全性、保密性和时效性而支付些许服务费用。

之前



之后

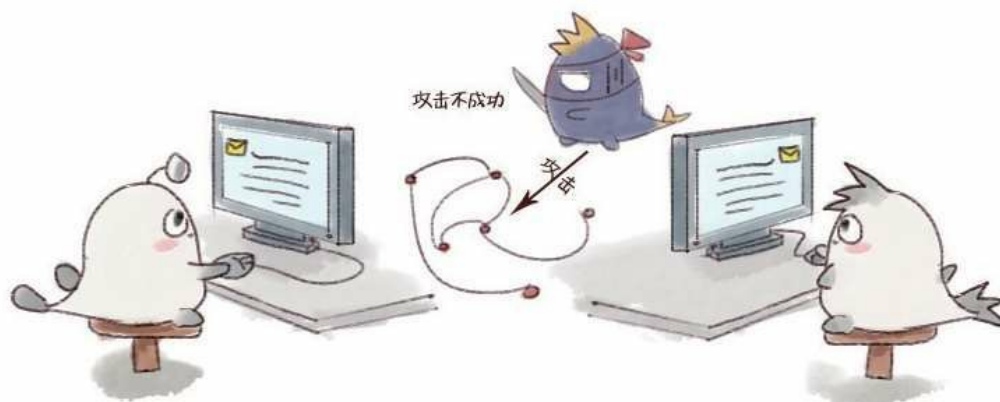


图4-46 区块链+电子邮件

综上，我们不难看出，区块链技术几乎可以渗透生活的每一个角落。也许20年、10年，甚至5年、1年后，区块链会以光速融入人们的生活。也许你也不知道具体哪里运用了区块链技术，但它已无处不在，与你的生活融为一体。

[1] 供应链金融 (Supply Chain Finance) [EB/OL]. [2017-05-18].<http://www.tceic.com/169959736i85ki3g86i2i522.html>.

[2] LendingRobot launches automated hedge fund secured by blockchain tech[EB/OL]. (2017-01-26) [2017-05-18].<http://venturebeat.com/2017/01/26/lendingrobot-launches-automated-hedge-fund-secured-by-blockchain-tech/>.

[3] Holberton School Begins Tracking Student Academic Credentials on the Bitcoinblockchain [EB/OL]. (2016-05-18) [2017-05-18].<https://bitcoinmagazine.com/articles/holberton-school-begins-tracking-student-academic-credentials-on-thebitcoin-blockchain-1463605176/>.

[4] Canada's SecureKey to Build a Blockchain Digital Identity Network with US Grant[EB/OL].

(2017-02-15) [2017-05-18].<https://www.cryptocoinsnews.com/canadas-securekey-to-build-blockchain-digital-identity-network-with-us-grant/>.

[5] Tech Giant Siemens is Now Working on BlockchainMicrogrids[EB/OL]. (2016-11-22) [2017-05-18].<http://www.coindesk.com/siemens-blockchainmicrogrid-lo3-ethereum/>.

[6] 全球首个能源区块链实验室成立 [EB/OL]. (2016-05-18) [2017-05-18].<http://news.bjx.com.cn/html/20160518/734100.shtml>.

[7] 区块链在政府方面的应用初解 [EB/OL]. (2016-08-17) [2017-05-18].<http://guba.eastmoney.com/news,cjpl,534320286.html>.

[8] Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents[EB/OL]. (2015-11-30) [2017-05-18].<https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offerblockchain-notarization-services-to-e-residents-1448915243/>.

[9] Block The Vote: Could Blockchain Technology Cybersecure Elections? [EB/OL]. (2016-08-30) [2017-05-18].<https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#1097f71b2ab>.

[10] 区块链技术在医疗领域应用分析[EB/OL]. [2017-05-18].<https://wenku.baidu.com/view/d551f47a6529647d2628524f.html>.

[11] Blockchain Startup to Secure 1 Million e-Health Records in Estonia[EB/OL]. (2016-03-03) [2017-05-18].<http://www.coindesk.com/blockchain-startupaims-to-secure-1-million-estonian-health-records/>.

[12] Australian Startup Cyph MD uses Blockchain Technology For Data Sharing in Healthcare[EB/OL]. (2016-08-09) [2017-05-18].<http://www.the-blockchain.com/2016/08/09/australian-startup-cyph-md-uses-blockchain-technology-datasharing-healthcare/>.

[13] Babyghost and VeChain: Fashion on the Blockchain[EB/OL]. (2016-10-18) [2017-05-18].<https://bitcoinmagazine.com/articles/babyghost-and-vechain-fashionon-the-blockchain-1476807653/>.

[14] Blockchain Going for a Song: New Tech Tunes Up Music Industry[EB/OL]. (2016-05-22) [2017-05-18].<https://cointelegraph.com/news/blockchain-going-for-asong-new-tech-tunes-up-music-industry>.

[15] Filament Nets \$5 Million for Blockchain-Based Internet of Things Hardware[EB/OL]. (2015-08-18) [2017-05-18].<http://www.coindesk.com/filamentnets-5-million-for-blockchain-based-internet-of-things-hardware/>.

[16] IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things[EB/OL]. (2015-01-17) [2017-05-18].<http://www.coindesk.com/ibm-revealsproof-concept-blockchain-powered->

internet-things/.

[17] “区块链+农业”落地不是梦[EB/OL]. (2016-10-28) [2017-05-18].<http://www.hooshong.com/news/133309.html>.

[18] 沃尔玛联合IBM和清华大学打造区块链试行项目[EB/OL]. (2016-10-20) [2017-05-18].http://www.sohu.com/a/116621490_448077.

[19] Blockchain Will Transform the Agriculture Industry[EB/OL]. (2016-09-06) [2017-05-18].<https://news.bitcoin.com/blockchain-agriculture-industry/>.

[20] 区块链：慈善腐败的克星[EB/OL]. (2016-11-28) [2017-05-18].<http://www.8btc.com/goodbye-corrupt-charities>.

[21] 2016年最具前景的五大区块链用例[EB/OL]. (2016-08-20) [2017-05-18].<http://www.8btc.com/five-ways-blockchain-2016>.

[22] 2016年最具前景的五大区块链用例[EB/OL].(2016-08-20) [2017-05-18].<http://www.8btc.com/five-ways-blockchain-2016>.

05 装备篇

装备拿好，从懵懂不解到自如对话

区块链是一个非常新的行业，严格来说，我进入区块链行业的时间并不长。在了解区块链技术之前，我的认知大多停留在：哦，区块链，新概念，大会的热点嘛，金融科技领域的厉害技术。

在我了解区块链技术的最初阶段，大致干了两件事。第一件就是恶补区块链历史上的一些典型事件和时间，并将其记在执行日历上，目的是不错过任何策划热点。那是一个夜黑风高的夜晚，比特币过生日了，我却忘记给它做张海报庆生。于是，半夜起来赶工海报的时候，我“幡然悔悟”并迅速捡起了这部分知识。本章第一部分的内容多为历史事实，我最初整理的时候引用了许多巴比特网站和一些国外比特币论坛上的资料，写作本书时又做了一些删减和补充。

第二件事，就是渐渐通过百度和知乎了解到讨论与区块链有关的话题时经常提起的词汇。我和这些词汇的最初接触，应该是在一次OKLink的内部讨论会上。那时我刚加入不久，会上一群小伙伴说着一些我完全听不懂的中英文词汇，一场会议下来，我听得云里雾里。因此，在本章的第二部分我主要罗列了一些并不是很核心，却是我最初接触区块链时听到和被提及的词汇。

比特币简史：从何处来往何处去

1975年4月5日 中本聪的生日

中本聪发布比特币白皮书的网站名为“P2P Foundation”，在该网站注册时有一个必须填写的项目：出生日期。而传说中的中本聪填写的日期就是1975年4月5日，当然，没有人知道这个信息究竟是不是真实的。

1982年 拜占庭将军问题

拜占庭将军问题，是由莱斯利·兰伯特（Leslie Lamport）等人提出的，这是一个点对点通信中的基本问题。其阐述的内涵是，在存在消息丢失的不可靠信道上试图通过消息传递的方式达成一致是不可能的。因此，对一致性的研究一般假设信道是可靠的，或不存在问题。而2008年出现的比特币区块链则解决了这个“历史遗留问题”。[\[1\]](#)

1	B	C	D
A	1	1	1

0	A	C	D
B	1	1	1

1	A	B	D
C	1	0	1

1	A	B	C
D	1	0	1

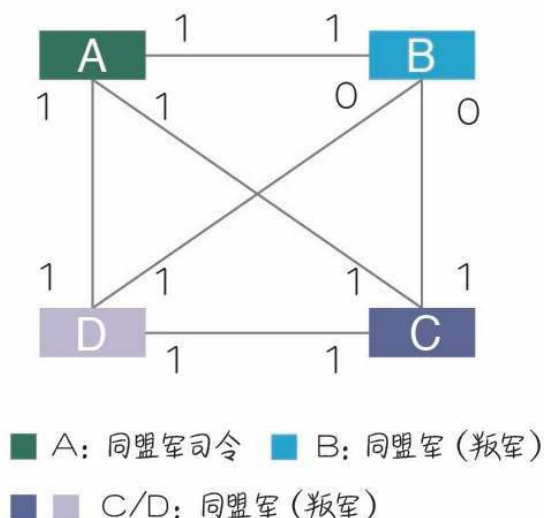


图5-1最简单的共识算法：拜占庭将军问题

1982年 密码学网络支付系统

戴维·乔姆（David Chaum）提出了注重隐私安全的密码学网络支付系统，该系统具有不可追踪的特性，被认为是比特币区块链在隐私安全方面的雏形。



图5-2 密码学网络支付系统

1990年Paxos算法被提出

Paxos算法也是莱斯利·兰伯特提出的，这是一种基于消息传递的一致性算法。Paxos算法解决的问题是一个分布式系统如何就某个值（决议）达成一致。[\[2\]](#)

	Backups	M/S	MM	2PC	Paxos
连续性	弱	最高		强	
交易	无	完全	本地	完全	
延迟	低			高	
吞吐量	高			低	中
数据丢失	很多	一些		无	
容错	向下	只读	读/写		

图5 - 3 Paxos算法与其他算法的对比

1991年 使用时间戳确保数位文件安全

斯图尔特·哈伯（Stuart Haber）与W. 斯科特·斯托尔内塔（W. Scott Stornetta）于1991年提出利用时间戳确保数位文件安全的协议，此概念之后被比特币区块链系统采用。

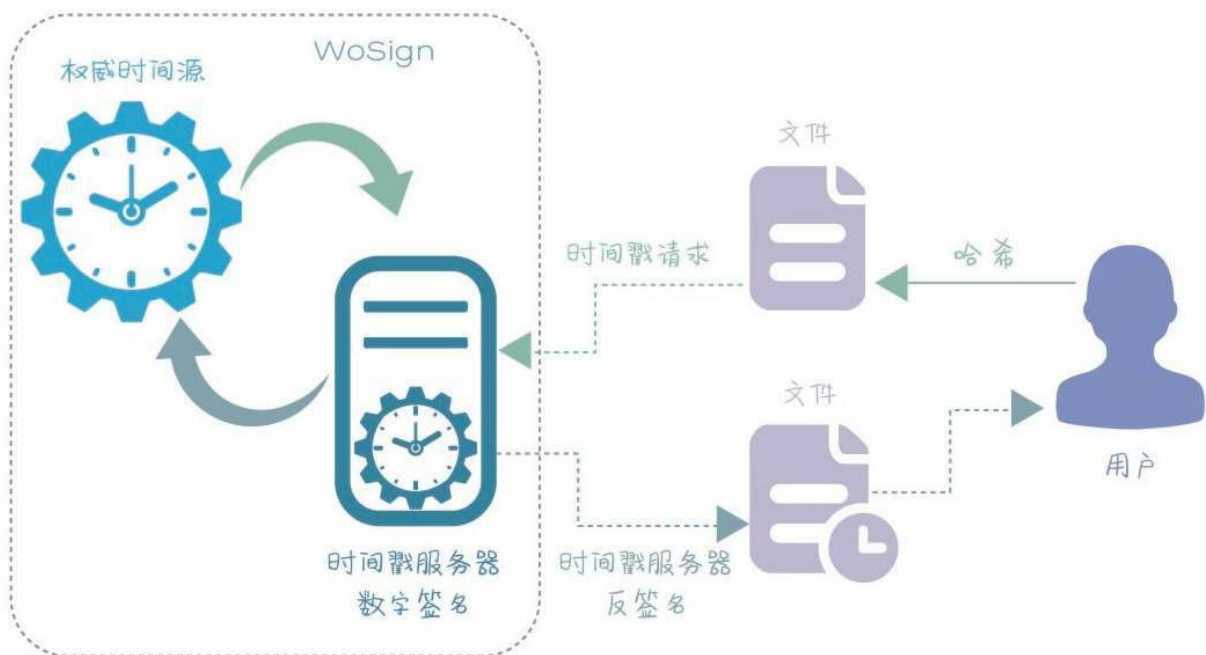


图5 - 4时间戳工作示意图

1997年 哈希现金技术被发明

亚当·巴克（Adam Back）发明的哈希现金是一种PoW演算法，此演算法依赖成本函数的不可逆特性，从而实现容易被验证但很难被破解的特性，最早被应用于阻挡垃圾邮件。哈希现金之后成为比特币区块链采用的关键技术之一。[\[3\]](#)

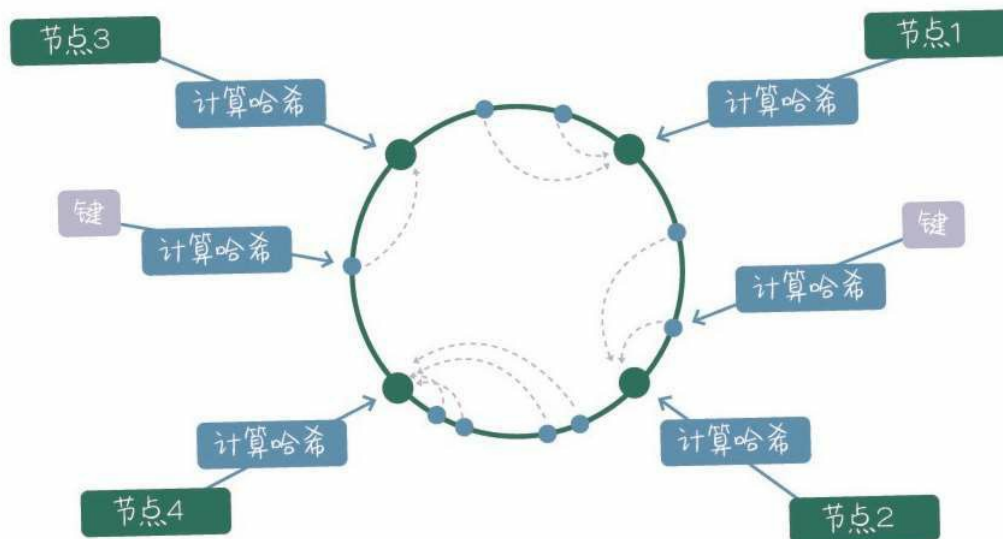


图5-5 哈希现金

1998年 分散式电子现金系统B-money

戴伟（Wei Dai）于1998年发表匿名的分散式电子现金系统B-money，引入PoW机制，强调点对点交易和不可篡改特性。

同年，尼克·萨博发表了去中心化的数位货币系统Bit Gold，参与者可贡献运算能力解出加密谜题。后来，哈尔·芬尼提出RPoW（可重复使用的工作量证明机制），将B-money与亚当·巴克提出的哈希现金结合起来创造了密码学货币。

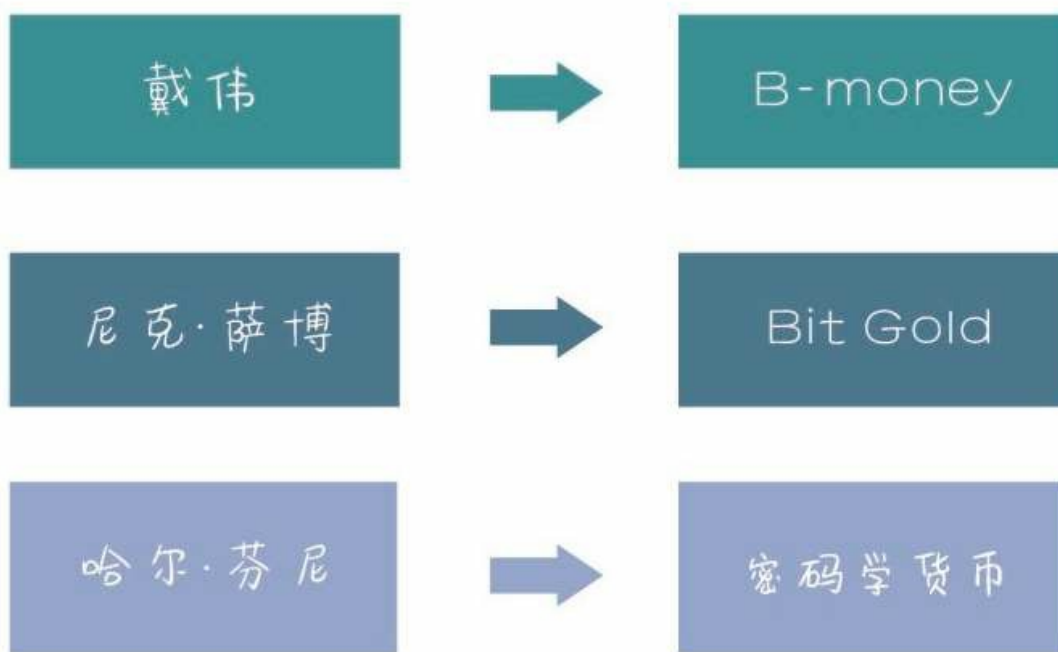


图5-6 电子货币

2008年11月1日 比特币白皮书发布

中本聪首先在《比特币：一种点对点的电子现金系统》（*Bitcoin: A Peer-to-Peer Electronic Cash System*）一文中提到了比特币。

2009年1月4日 创建“创世区块”

北京时间2009年1月4日02:15:05，中本聪创建了比特币世界的第一个区块——“创世区块”，新版本的比特币系统将它设定为0号区块，而旧版本的比特币系统将它设定为1号区块。

交易

交易时间	2009-01-04 02:15:05
所属区块	0

图5-7 创建“创世区块”

2009年1月11日 比特币客户端0.1版发布

2009年1月11日，中本聪发布了比特币客户端0.1。这是比特币历史上的第一个客户端，它意味着更多人可以挖掘和使用比特币了。



图5-8 比特币客户端0.1版发布

2009年1月12日 第一笔比特币交易

2009年1月12日，中本聪将10枚比特币发送给开发者、密码学活动分子哈尔·芬尼。这是比特币历史上的第一笔交易。

区块 #170

时间	2009-01-12 11:30:25
难度	1.000
交易数	2
总转出量	100 比特币
奖励	50 比特币

图5-9 第一笔比特币交易

2009年10月5日1美元=1 309.03比特币

最早的比特币与美元的汇率为1美元=1 309.03比特币，由一位名为“新自由标准”（New Liberty Standard）的用户发布。一枚比特币的价值计算方法如下：由高CPU（中央处理器）利用率的计算机运行一年所需要的平均电量1 331.5千瓦时，乘以上年度美国居民平均用电成本0.113 6美元，除以12个月，再除以过去30天里生产的比特币数量，最后除以1美元。

1.00 美 元	=	885.91 比 特 币	10/13/2009
1.00 美 元	=	907.40 比 特 币	10/12/2009
1.00 美 元	=	867.02 比 特 币	10/11/2009
1.00 美 元	=	892.52 比 特 币	10/10/2009
1.00 美 元	=	833.02 比 特 币	10/09/2009
1.00 美 元	=	922.27 比 特 币	10/08/2009
1.00 美 元	=	952.02 比 特 币	10/07/2009
1.00 美 元	=	1 130.53 比 特 币	10/06/2009
1.00 美 元	=	1 109.03 比 特 币	10/05/2009

图5 - 10 比特币的汇率

2009年12月30日 比特币挖矿难度首次增长

为了保持每10分钟1块的恒定开采速度，比特币网络进行了自我调整，挖矿难度变得更大。2009年12月30日，比特币挖矿难度首次增长。

区块 # 32255

时间	2009-12-30 13:58:59
难度	1.000

区块 # 32256

时间	2009-12-30 14:11:04
难度	1.182

图5 - 11比特币挖矿难度首次增长

2010年7月12日 第一次价格剧烈波动

2010年7月12—16日，比特币汇率经历了为期5天的价格剧烈波动时期，从0.008美元/比特币上涨到0.080美元/比特币，这是比特币汇率发生的第一次价格剧烈波动。

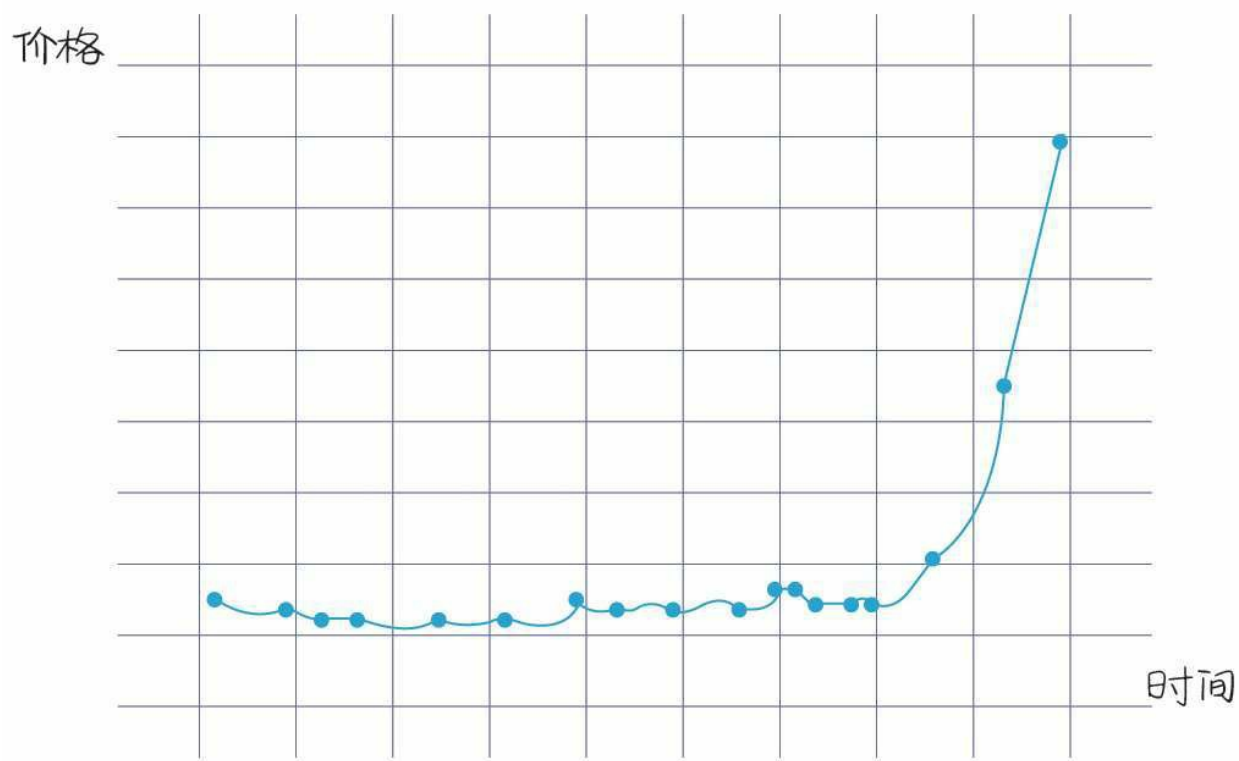


图5 - 12 第一次价格剧烈波动

2010年7月12日GPU挖矿开始

由于比特币的汇率持续上升，积极的矿工们开始寻找提高计算能力的方法。专用的图形卡比传统的CPU具有更多的能量。据称，矿工ArtForz是第一个成功实现在矿场上用个人的OpenCL（开放运算语言）GPU（图形处理器）挖矿的人。[\[4\]](#)



图5 - 13 GPU挖矿

2010年8月6日 比特币网络协议升级

比特币协议中的一个主要漏洞于2010年8月6日被发现：交易信息未经正确验证，就被列入交易记录或区块链。这个漏洞被人恶意利用，生成了1 840亿枚比特币，并被发送到两个比特币地址上。这笔非法交易很快就被发现，漏洞在数小时内修复，非法交易被从交易日志中删除，比特币网络协议也因此升级至更新版本。[\[5\]](#)

2010年10月16日 第一笔托管交易

比特币论坛会员Diablo-D3和Nanotube于2010年10月16日进行了第一笔有记录的托管交易，托管人为theymos。

2010年12月5日 比特币第一次与现实的金融社区产生交集

在维基解密泄露美国外交电报事件期间，比特币社区呼吁维基解密接受比特币捐款以打破金融封锁。中本聪表示坚决反对，认为比特币还在摇篮中，经不起冲突和争议。

2010年12月16日 比特币矿池出现

采矿成为一项团队运动，一群矿工于2010年12月16日一起在slush矿池挖出了它的第一个区块。根据其所贡献的工作量，每位矿工都获得了相应的报酬。此后的两个月间，slush矿池的算力从1 400 Mhash/s增长到了60Ghash/s。[6]



图5 - 14比特币矿池出现

2011年6月20日Mt. Gox出现交易漏洞

世界上最大的比特币交易网站Mt.Gox（也作MtGox）于北京时间2011年6月20日午夜挂出了令人震惊的行情，1比特币只卖1美分，而此前的正常价格在15美元左右。Mt.Gox一方面号召用户赶紧修改密码，另一方面宣布这一反常时段内的所有大单交易无效。

2011年6月29日 比特币电子钱包

比特币支付处理商BitPay于2011年6月29日推出了第一个用于智能手机的比特币电子钱包。同年7月6日，一个免费的比特币数字钱包App现身安卓应用商店，这是第一款与比特币相关的智能手机和平板电脑App。该App由布兰登·伊利斯（Brandon Iles）研发。[\[7\]](#)

2011年7月 比特币悬案

2011年7月，当时世界第三大比特币交易所Bitomat宣布，他们丢失了wallet.dat文件的访问权限，也就是说他们丢失了代客户持有的17 000枚比特币。

2011年11月10日 比特币POS（销售终端）研制成功

比特币POS与互联网相连，由一个128×64像素的背光单色显示器、收据打印机，以及一个24键的键盘组成，此外还包括一个USB（通用串行总线）接口，可以连接QR（快速反应）条码扫描仪。[\[8\]](#)



图5 - 15 比特币POS界面

2012年8月14日 芬兰中央银行承认比特币的合法性

2012年8月14日，当一名芬兰广播电视台的记者询问一名芬兰中央银行的代表比特币具有哪些法律地位时，该代表回复说：“我们并没有做出任何比特币能够兑换官方货币的保证。像比特币这样不受（政府）管理的虚拟货币不存在这样的保证。”记者接着问道：“难道比特币不合法吗？”代表回应道：“根本不是这么一回事，人们可以使用任何他们喜欢的货币做投资。毕竟芬兰是一个自由的国度。”



图5-16 芬兰中央银行承认比特币的合法性

2012年9月27日 比特币基金会成立

为了实现规范、保护和促进比特币发展的目标，比特币基金会成立了。该基金会对于媒体和企业发起的符合相关法规的查询具有重大的意义。

2012年11月28日 区块奖励首次减半

比特币挖矿的奖励从之前的每10分钟50枚比特币减至25枚比特币，区块#210000是首个奖励减半的区块。

Block Mtea BTC	
区块 #210000 主链	
时间	2012-11-28 23:24:38
难度	3438 361 434
交易数	457
总转出量	2542170093021 比特币
奖励	25 比特币

图5 - 17 区块奖励减半

2013年10月25日FBI成为比特币新富豪

海盗罗伯茨的传奇生涯可能要画上句号了，FBI（美国联邦调查局）控制了其账户上的144 000枚比特币，并将这些比特币转移到了FBI控制的比特币地址上。[\[9\]](#)



图5 - 18 FBI成为比特币新富豪

2013年11月29日 比特币价格首度超过黄金

2013年11月29日，比特币在Mt.Gox上的交易价格达到1 242美元/比特币，同一时间的黄金价格为1 241.98美元/盎司，比特币价格首度超过黄金。



【更多新书朋友圈免费首发，微信jrgh3w】

图5-19 比特币价格首度超过黄金

2013年12月5日 中国五部委发通知

2013年12月5日，中国人民银行等五部委发布《关于防范比特币风险的通知》，明确比特币不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。通知发出后，当天比特币的单价大跌。

2013年12月18日 比特币单价暴跌

2013年12月18日，中国两大比特币交易平台比特币中国和OKCoin发布公告，宣布暂停人民币充值服务。随后，比特币的单价跌到了2011元人民币。[\[10\]](#)

各位亲爱的比特币中国用户：

由于众所周知的原因，比特币中国不得不暂时停止人民币充值服务，比特币充值、比特币提现和人民币提现不受影响，比特币中国会继续运营。请大家继续关注我们的主页，我们会尽快提供其他的充值途径。给您带来的不便，我们在此表达深深的歉意。

比特币中国

2013.12.18

图5 - 20 比特币单价暴跌

2014年7月9日 波兰财政部确认比特币作为一种金融工具

2014年7月9日，波兰财政部副部长沃伊切赫·科瓦尔奇克（Wojciech Kowalczyk）发布了一个文件，确认了比特币在波兰现有的金融法规下可作为一种金融工具。

财政部回应说：

“

根据金融工具法案，比特币可以被看作金融工具。

”

明确比特币的合法地位

在通知中，科瓦尔奇克证实了比特币在波兰并非是一种官方认可的货币，他在文件中指出：

“

根据国家法规分析得出的结论是，比特币并非由法律界定并被普遍接受的货币，因此它不能被归类为一种国家货币或者外币。

”

图5-21 波兰财政部发言

2014年7月12日 法国发布比特币新规

2014年7月12日，法国经济和金融部门表示将在当年年底对比特币和其他数字货币的金融机构和个人使用者实施监管措施。“虽然目前虚拟货币的体量不可能对经济体系产生影响，但这些非官方的货币正在发展，并且存在非法或者欺诈的风险。”

文件提出：

“我们已经提议设立一个5 000欧元的利润税门槛。我们认为在征税之前，法国政府应该允许人们尝试用比特币投资和发展商业活动。”

图5 - 22 法国发布监管新规

2014年12月11日 微软接受比特币支付

全球计算机巨头微软于2014年12月11日宣布接受比特币作为一种支付选项，允许消费者用比特币购买其在线平台上的各种数字内容。根据微软官方商店的支付信息页面，美国的消费者可以用比特币为他们的微软账户充值。[\[11\]](#)

2015年10月22日 欧盟对比特币免征增值税

欧盟法院于2015年10月22日裁定，对于比特币及其他虚拟货币的交易将免征增值税。这一决定对于比特币交易群体而言，将是一次重大的胜利，因为这意味着，他们在接下来的虚拟货币交易中，将无须缴税。[\[12\]](#)

2015年12月16日 比特币证券发行

2015年12月16日，美国证券交易委员会批准在线零售商Overstock通

过比特币区块链发行该公司的股票。据Overstock提交给证券交易委员会的S-3申请，该公司希望通过区块链发行最高5亿美元的新证券，包括普通股、优先股、存托凭证、权证、债券等。[\[13\]](#)

2016年4月5日OpenBazaar上线

去中心化电子商务协议OpenBazaar的开发者于2016年4月5日发布其首个正式版本软件。OpenBazaar能够让点对点的数字商务成为可能，并使用比特币作为一种支付方式，类似于一个去中心化的“淘宝”。[\[14\]](#)

2016年5月25日 日本认定比特币为财产

日本参议院于2016年5月25日批准了一项监管国内数字货币交易所的法案，法案将比特币归类为一种资产或财产。

2016年6月 民法总则划定虚拟资产保护范围

第十二届全国人大常委会第二十一次会议于2016年6月在北京举行，会议首次审议了全国人大常委会委员长提请的《中华人民共和国民法总则（草案）》议案的说明。草案对网络虚拟财产、数据信息等新型民事权利客体做出了规定，这意味着网络虚拟财产、数据信息将正式成为权利客体，比特币等网络虚拟财产将正式受到法律保护。[\[15\]](#)

2016年7月20日 比特币奖励二次减半

第420000个比特币区块已被开采完毕，区块奖励于2016年7月20日迎来了第二次减半，成功降至12.5比特币。由于之前的减半发生在第210000个区块，当时的货币通货膨胀率从12.5%下降到了8.3%，而此次奖励减半发生在第420000个区块，将通货膨胀率降至4.17%，所以接下来的奖励减半将发生在第630000个区块，时间约为4年之后。[\[16\]](#)

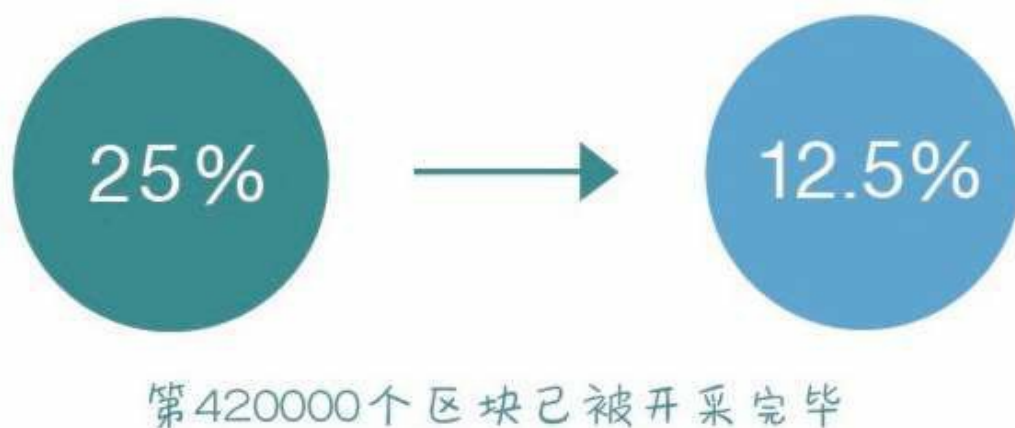


图5 - 23 比特币奖励二次减半

2017年2月 中国央行数字货币试运行

中国央行或将成为全球首个发行数字货币并将其投入真实应用的中央银行。据悉，央行推动的基于区块链的数字票据交易平台已测试成功，由央行发行的法定数字货币已在该平台试运行。[\[17\]](#)

区块链词条：人手必备拿好不送

区块链

这个词可以说是必备词汇了，很多人更倾向于叫它的英文名字：**blockchain**。而在最近的一次投票中，它又被“公投”成了“公信链”，不过目前为止提到最多的仍然是区块链。它是比特币的底层技术，是一个去中心化的分布式账本系统。区块链与人工智能、大数据并称金融科技的三大巨头。

比特币

这个词差不多是区块链领域中被提及最多的了。比特币是区块链技术的第一个落地应用，最早是一种**P2P**形式的网络虚拟货币，但是在很多国家，它已经可以购买现实生活中的物品了。如今，比特币已发展成为根据中本聪的思路设计发布的开源软件以及建构其上的**P2P**网络。

中本聪

这是一个在探索区块链领域的过程中必然会遇到的词汇，它是一个人名，是比特币的开发者兼创始人。2008年，中本聪在一个讨论信息加密的邮件组中发表了一篇文章，勾画了比特币系统的基本框架。2009年，他为该系统建立了一个开放源代码项目，正式宣告了比特币的诞生。当比特币渐成气候时，中本聪却悄然离去，从互联网上销声匿迹。

许多比特币的“纪念日”都和中本聪有关。

数字货币

区块链最初的应用形式就是数字货币。数字货币是电子形式的替代货币，数字金币和密码货币都属于数字货币。它不能完全等同于虚拟世界中的虚拟货币，因为它经常被用于真实的商品和服务交易，而不仅仅局限在网络游戏等虚拟空间中。目前全世界共有数千种数字货币。

PoW

当热爱学习的你想要再深入一点了解区块链的原理时，这个词一定会出现。PoW，也就是工作量证明。比特币在区块的生成过程中使用了PoW机制。一个符合要求的区块哈希值由N个前导零构成，零的个数取决于网络的难度值。要得到合理的区块哈希值需要经过大量的尝试计算，计算时间取决于机器的哈希运算速度。[\[18\]](#)

公钥和私钥

在有关区块链的话题中，我们还会经常听到这两个词汇：公钥和私钥。这就是俗称的不对称加密方式，是对以前的对称加密（使用用户名与密码）方式的提高。

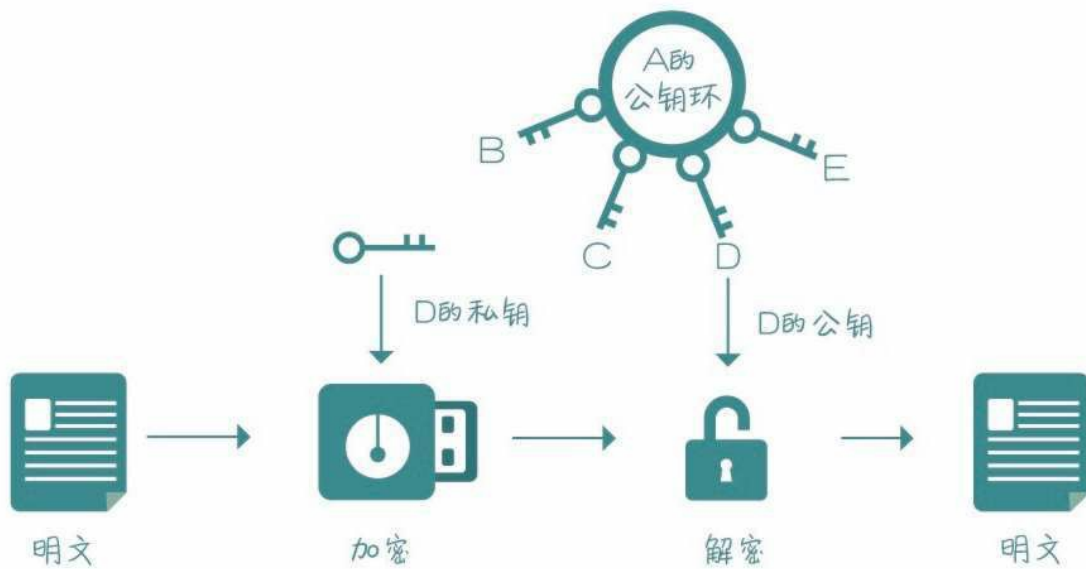


图5 - 24 不对称加密

在比特币系统中，私钥本质上是由32个字节组成的数组，公钥和地址的生成都依赖私钥，有了私钥就能生成公钥和地址，就能够使用对应地址上的比特币。

哈希值

这个词在比特币的世界中可以说是无处不在，哈希算法将任意长度的二进制值映射为固定长度的较小二进制值，这个小的二进制值就是哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。哪怕只更改一段明文中的一个字母，随后产生的哈希值都将千差万别。要找到对应同一哈希值的两个不同的输入，从计算的角度来说基本上是不可能的。[\[19\]](#)

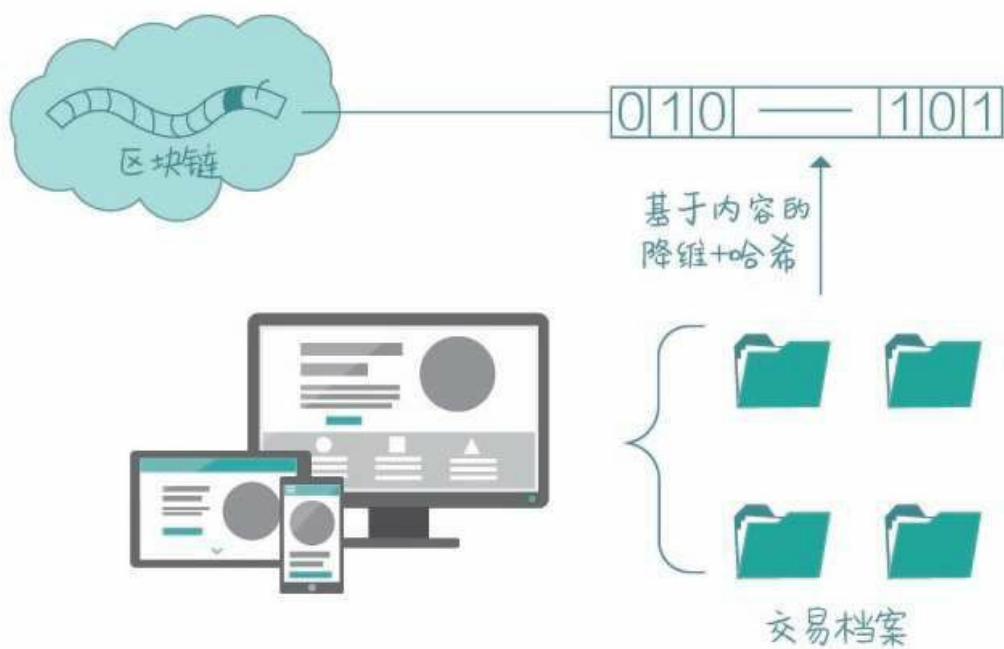
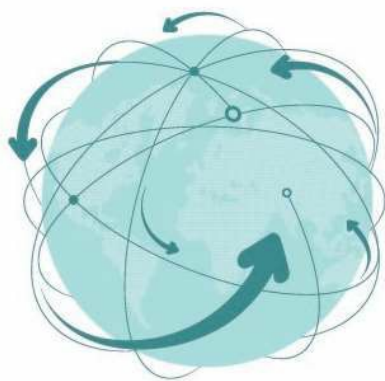


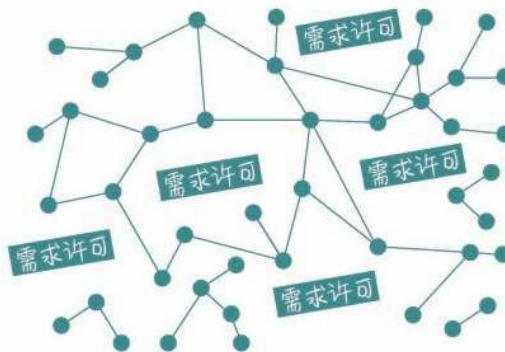
图5 - 25 区块链的降维+哈希

公有链和私有链

业内人士总会被问及这样的问题：听说你对区块链“一知半解”，来来，帮我分分类，这个应用是公有链还是私有链？



公有链：对所有人开放，
任何人都可以参与



私有链：对单独的个人
或实体开放

图5-26 公有链和私有链

公有链是指全世界任何人都可读取、任何人都能在其中发送交易信息且交易能够获得有效确认、任何人都能参与共识过程的区块链——共识过程决定哪个区块可被添加到区块链中，也能让参与者明确当前状态。公有链通常被认为是完全去中心化的。而私有链是指其写入权限仅在一个组织手中的区块链。

概括来说，公有链对所有人开放，任何人都可以参与；私有链只对单独的个人或实体开放。[\[20\]](#)

区块和链

区块指的是信息块，每个区块都包含三个要素：本区块的ID；若干交易单；前一个区块的ID。

比特币系统大约每10分钟就会创建一个区块，其中包含了这段时间里全网范围内发生的所有交易。每个区块中也包含了前一个区块的ID，

这使得每个区块都能找到它之前的那个节点，这样一直倒推就形成了一条完整的交易链条。从诞生之初至今，全网形成了一条唯一的主区块链。

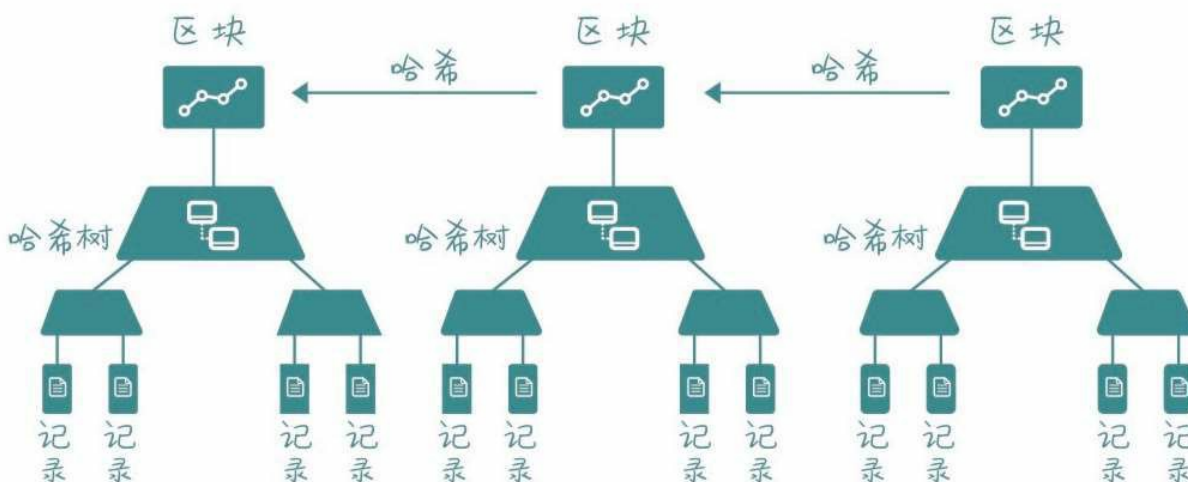


图5 - 27 区块和链

智能合约

智能合约也是我们时常听到的词汇，而且听起来似乎可以理解又不可以理解，按照字面意思来看，就是一个自动自觉执行的、有点聪明的合同吧。

智能合约的发明者尼克·萨博将其定义如下：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”[\[21\]](#)

智能合约利用程序算法替换执行合同，杜绝了执行主体和交易的道德风险。



图5-28 智能合约

信用共识

这个词多次出现在有关区块链的报道和会议上。只要被问到区块链能干什么、区块链为什么会改变世界、区块链有什么用这些问题时，信用共识这个词就会出现。

区块链的分布式结构以及基于数学算法的低成本信任机制，为金融领域相关问题的解决和优化提供了一种新思路 and 路径。目前经济社会中的信用环境比较弱，信用成本比较高，而区块链技术提出了一套成本较低的信任解决方案，对促进信用经济的发展具有重要意义。



图5 - 29 区块链信用共识

R3

R3区块链联盟涵盖了70多家全球顶尖金融机构，包括来自中国的中国平安集团、招商银行、中国外汇交易中心、民生银行等4家传统金融机构，目标是打造金融机构的私有区块链系统。

2016年5月，R3开始为旗下的分布式账本联盟寻求2亿美元的A轮融资，R3自身持股10%。随后，R3将目标融资金额下调到1.5亿美元，R3自身持股升至40%，剩余60%股份，则计划主要向联盟42家初始会员银行募集，其后，7家银行选择退出融资。继R3宣布将其开发的区块链平台Corda开源后，包括高盛在内的一些成员退出了R3联盟。[\[22\]](#)

[\[1\]](#) 区块链技术演进史[EB/OL]. (2016-04-25) [2017-05-18].<http://tech.hexun.com/2016-04-25/183507891.html>.

[\[2\]](#) 分布式一致性算法——Paxos [EB/OL]. (2016-06-27) [2017-05-18].<http://www.cnblogs.com/cchust/p/5617989.html>.

[\[3\]](#) BTC电子货币系统背后的技术 [EB/OL]. (2013-12-20) [2017-05-18].<http://it.dataguru.cn/article-3986-1.html>.

- [4] 比特币的五年历程(全文更新完) [EB/OL]. (2016-08-13) [2014-01-08].<http://8btc.com/thread-2603-1-1.html>.
- [5] 协议漏洞产生1 840亿枚比特币 [EB/OL]. (2010-08-15) [2017-05-18].<http://www.8btc.com/184-billion-bitcoins>.
- [6] 比特币：数字时代的“挖矿”江湖[EB/OL]. (2017-03-03) [2017-05-18].<http://www.fx361.com/page/2017/0303/922619.shtml>.
- [7] BitPay推出比特币电子钱包[EB/OL]. (2011-06-29) [2017-05-18].<http://www.8btc.com/bitpay-launches-e-wallet>.
- [8] 比特币销售终端 (POS) 研制成功 [EB/OL]. (2011-11-10) [2017-05-18].<http://www.8btc.com/bitcoin-pos>.
- [9] FBI得到丝绸之路的比特币成为新首富[EB/OL]. (2013-10-25) [2017-05-18].<http://www.8btc.com/fbi-ross-ulbricht-2>.
- [10] 比特币退出中国？交易平台暂停人民币充值[EB/OL]. (2013-12-19) [2017-05-18].<http://www.kejixun.com/article/201312/27153.html>.
- [11] IT巨头微软将比特币列为支付选项[EB/OL]. (2014-12-11) [2017-05-18].<http://www.8btc.com/microsoft-adds-bitcoin-payments-xbox-games-mobile-content>.
- [12] 欧盟法院裁定数字货币交易将免征增值税 [EB/OL]. (2015-10-22) [2017-05-18].<http://www.8btc.com/bitcoin-is-exempt-from-vat>.
- [13] Overstock或通过区块链技术发行最高5亿美元新证券[EB/OL]. (2015-12-16) [2017-05-18].<http://www.btc38.com/btc/altgeneral/8982.html>
- [14] 4月4-10日这周数字货币圈都发生了什么大事？ [EB/OL]. (2016-04-10) [2017-05-18].<http://mt.sohu.com/20160410/n443807602.shtml>.
- [15] 法律保护虚拟财产公告[EB/OL]. (2016-06-29) [2017-05-18].<http://www.cnfla.com/gonggao/50131.html>.
- [16] 比特币产量成功迎来第二次减半，价格波动剧烈[EB/OL]. (2016-07-10) [2017-05-18].http://www.8btc.com/halving_megathread_block.
- [17] 央行数字货币真的来了业界点赞同时仍有问题待解 [EB/OL]. (2017-02-09) [2017-05-18]. http://www.cs.com.cn/xwzx/jr/201702/t20170209_5172817.html.
- [18] 比特币原理 [EB/OL]. (2014-01-26) [2017-05-18].<http://blog.csdn.net/autumn84/article/details/18782533>.
- [19] Hash值是什么[EB/OL]. [2017-05-18].<http://product.pconline.com.cn/itbk/software/dnwt/1504/6325876.html>.
- [20] 全面认识区块链：公有链vs私有链[EB/OL]. (2016-08-09) [2017-05-18].

<http://www.weiyangx.com/199778.html>.

[21] 什么是智能合约? [EB/OL]. (2014-12-14) [2017-05-18].[http://www.8btc.com/ what-are-smart-contracts-in-search-of-a-consensus](http://www.8btc.com/what-are-smart-contracts-in-search-of-a-consensus).

[22] 融资激化R3区块链联盟分歧 高盛、摩根斯坦利、摩根大通等7家银行退出[EB/OL]. (2016-11-29) [2017-05-18].http://www.sohu.com/a/120161115_115035.

附录

在区块链创业公司做COO是一种什么体验？

OKCoin币行& OKLink COO潘晓军

COO（首席运营官）是创业公司永不停歇的发动机，不但自带光环，还要点燃他人。他的日常工作，是这个样子的。

人才、人才、人才——重要的事情说三遍

靠谱的人做靠谱的事，没有优秀团队的区块链创业公司就像是没有根基的大树，风一吹就倒。区块链创业公司和其他互联网公司一样也会围绕人才和战略展开。战略生成产品，产品获取市场，市场捕获用户的芳心，最终挣得收入和利润。但比起其他互联网公司，区块链创业公司引进优秀人才的需求更加迫切，要求也更高。区块链技术是一个快速发展的应用领域，需要那些敢于冒险、胆大心细、坚韧不拔的伙伴去探索新知。优秀的区块链公司，本身就是一个充满价值节点的网络，产品、开发、测试、市场、运营各种各样的人才缺一不可。COO需要做的首先是源源不断地筛选出优秀人才，组建好团队，这样才能共同奏响企业发展的乐章。

“21世纪最重要的是什么？人才！”

区块链创业公司，也是这样！

确保目标实现的老司机

人员齐备后，志同道合的小伙伴们就登上了一条需要同心协力才能开动的大船。公司的CEO会制定好目标，而目标的实现则需要COO的把控。每周的管理例会、每季度的绩效评估和反馈、年度以及不定期的股东会议，都将确保小伙伴们时时就位，朝着同一个目标努力。

产品、市场、运营三军齐努力

“区块链是什么？能不能一句话讲给我听。”

“哦，明白了，但这和你们有什么关系呢？”

“你们的数字资产交易平台会不会跑路，你们提供的跨境支付服务有西联汇款好用吗？”

“我的账户转账怎么还没到？”

“天呐，K线又断了！”

“央行又发文了，你们怎么看？”

.....

不停应对用户的各类问题，这也是COO的日常。

此外，COO还要做市场研究：菲律宾和马来西亚的监管有什么特色？最近手机端的点击量和装机率为什么下降这么多？

也就是说COO不仅要倾听用户的声音，还要观察市场的脸色，当然还有更重要的：“拉新、留存和激活”。不论是线上的合作渠道、媒体的

推广，还是线下的商务、品牌、政府和公关合作，甚至使用什么样的策略达到目标效果，这些事情都需要COO组织各个部门合力完成。

COO可能是公司最操心的人，“上得厅堂定战略，下得厨房做执行”，享受挑战和解决问题的人才适合做COO。

区块链公司的“技术大牛”们是不是都怀着改变世界的梦想？

OKLink产品经理兼首席工程师 于亮

区块链，我第一次听到这个词汇大概是2013年年初。作为一个从事互联网技术研发的人，我带着一颗好奇心查看了当时所有能查阅到的中英文资料，尽管我的英文水平有限，但我还是想理解原汁原味的区块链技术原理。如今，大家把区块链当作一种技术，当时的我也认为区块链一定带有技术的属性，我也正是从这个角度进一步学习了这项所谓的“技术”。下面我将遵循学习的三部曲——是什么、为什么、怎么做，从这三个方面聊一聊我对区块链的理解。

首先，区块链到底是什么？现在各大主流媒体都在讲区块链技术，把区块链定位成一项技术。我不太认同这个定位，我认为区块链这个新事物更像是一套针对信用问题的解决方案。

我们都知道现在全世界的信用体系无外乎以下几种：第一，基于道德，靠道德约束解决信用问题。比如我们去饭店吃饭，因为信息不对称，我们不知道饭店老板是不是用了地沟油，是不是用了不太健康的食材。但我们选择信任饭店老板，认为饭店老板不会做出有害顾客身心健康的事情。第二，基于信仰。以前听过一个笑话说西方很少出现食品安全问题，一个很大的原因是从事食品生产的人害怕上帝的惩罚。因为大家都相信上帝，相信上帝是公平的裁判，于是靠着这样一种信仰，人们建立起一套信用体系。第三，基于政府。说到政府我们不得不谈到世界上每一个国家的银行体系，可以说它们都建立于政府的基础上。每一位公民都认为自己的政府不会垮掉，任何时候政府都是人民强大的后盾。只要政府不垮台，老百姓存在银行户头上的数字就有价值，就可以作为

商品交换的媒介。

区块链出现之后，世界上又多了一种新的信用体系的基石——算法。算法一词源于计算机世界里的一个概念，算法有一个特性，那就是一致性。不论时间、地点，只要输入确定，经过算法，输出就一定确定，这就是算法的一致性的基本定义。

区块链正是基于这种特性建立起来的一种新型信用体系。

其次，为什么选择区块链。因为区块链有以下几大特性：第一，安全。从技术角度说，区块链在本质上是一个分布式的数据库，每一个数据节点都储存着这个分布式系统中全部数据的副本。也就是说，每个数据节点都独立记录区块链世界里的每一笔交易。当一笔交易发生，系统会通过P2P协议，将交易广播到区块链中的每一个数据节点。举个例子，比如区块链里有100个人，其中一个人向另外一个人转了一笔钱，转款人担心收款人撒谎说未收到汇款，于是转款人就给除自己之外的所有人发了一封邮件，附带汇款账单和亲笔签名。因为有99个人可以为转款人证明，所以收款人也就无法作假了。

第二，稳定。之前听到过这样一句话：即便美国总统奥巴马有再大的权力，他也不能摧毁区块链。作为区块链最成熟的运用，比特币区块链中有成千上万个数据点，遍布世界各地。比特币协议将各个节点组织成了一个强大的比特币区块链网络，所以说区块链很难被某个人或某个组织摧毁。

最后，选择区块链做什么？现在的比特币区块链已经可以做到点对点支付。比如说你想给美国的一个朋友汇一笔钱，按照传统处理方式，需要到银行柜台办理，由银行通过国际汇款通道SWIFT将汇款转入美国，再由美国当地的银行投递给你的朋友。这样的传统汇款方式有以下几个弊端：汇款手续费高昂，汇款周期长，汇款过程不透明。通过区块链可以真正做到点对点汇款，到账周期短，并且信息公开透明、可以实

时查询。

目前，OKLink正在致力于构建一个基于区块链的全球汇款网络。针对传统汇款方式的弊端，OKLink设计了一套可以实时到账、低手续费、汇款信息可全程追踪的全球汇款网络，现已在加拿大、韩国、日本、菲律宾、印度、越南、印度尼西亚、新加坡、中国台湾、中国香港等国家和地区开通汇款业务，基本可以做到实时到账。很神奇，不是吗？

我相信区块链带来的技术革新将会对每一个行业产生颠覆性的影响，让我们翘首以待吧。

想要让你看懂抽象化的区块链我可能还差**100**个毕加索！

OKCoin币行& OKLink设计总监 李超

区块链伴随着比特币等加密货币诞生，是一种存储数据的独特方式。近年来，关于区块链的创新应用与设计层出不穷。对于不在专业领域的我们来说，通过文字似乎总是无法感受到区块链的强大魅力。

自2013年起，区块链不断发展，这让总是喜欢研究新事物的设计师们产生了极大兴趣。我总是在想，与枯燥的数据与笼统的文字解释相比，融入相关设计元素的可视化图像是不是更加直观有趣呢？对于经常接触传统数据的我们来讲，这无疑也是一种新的尝试与挑战，而区块链技术本身的复杂性也给设计工作增加了一定难度。

想要做好它，先要了解它！

简约的设计并不代表设计过程是简单的，设计师们想要以简洁明了的形式对区块链进行视觉化设计，这个过程并不容易。在设计前期，我们将设计驾于数据之上，追求本心，根据呈现方式考虑解决方案。应用Python（面向对象的解释型计算机程序设计语言）相关套件，我们理解了区块链的原理，领会了交易历史无法被改写这一概念，这种将银行排除在外、而在公开网络上采用可验证的分布式账本系统验证交易的技术让我们叹为观止。在分析理解了区块链的原理之后，我们决定使用JavaScript（直译式脚本语言）函式库D3.js，D3的图标类型非常丰富，并且支持SVG格式，用其构建的数据图表非常强大，我们可以利用它的丰富特性充分表现区块链的复杂性，具有极佳的视觉表现效果。在设计后期，我们将设计与数据结合。视觉开发需要从简单的资料开始，比如

区块#235235内记载了834笔交易，这么大的交易量在视觉表现上会有一定难度，为了使整体的视觉设计不受数据变化的影响，要向数据靠拢。设计师的目的是通过简洁明了的视觉化设计使过程变得简单明了，例如在交易过程中，发送方与接收方都可通过视觉化系统对交易流向进行追踪。

视觉化的展示降低了解区块链的门槛，希望大家在看到图表时能恍然大悟：“哇，原来区块链也不是一个很难理解的概念。”区块链的确不是什么新技术，只是技术人员赋予了它很多专业术语，让其变得晦涩难懂。

为了推广没人知道的区块链我们做了哪些疯狂的事？

OKCoin币行& OKLink品牌公关总监 田颖

区块链是一种全新的东西，有着全新的底层技术、上层应用以及运行原理，除了互联网，历史上还从来没有过这样的东西。试图给大众讲清楚区块链到底是什么，就像给20世纪80年代的人讲解互联网是什么东西一样困难。

如果你告诉20世纪80年代的人们可以在互联网上购物，他们会有什么样的反应？

- 谁会愿意在网上买衣服？别说梦话了。
- 网上买衣服试都没法试，靠一张图片就要我付钱？
- 一定是骗子，想骗钱想疯了吧。

如果你向他们介绍谷歌，他们会有什么样的反应？

- 免费搜索？那他们怎么赚钱？一定是套路！
- 这样的公司市值5 000亿美元？就能查个信息值这么多钱？
- 就这样一个简单的页面网站需要5万多名员工？人工搜索？

那如果你要告诉现在的人们，有一个程序员写了一段可以改变整个金融市场格局的程序，他们会有什么样的反应？

- 炒概念圈点钱罢了，用不了几天就销声匿迹了。

- 没有权威政府背书，就靠一段代码做公正，疯了吧。
- 一定有黑客在背后操作系统，人为制造的就一定能人为操控！

这些话听起来是不是都很有道理、逻辑严谨、无法反驳？这就是我们遇到的问题。

在过去的一年里，我们奔赴全国多个城市，做了数十场线下活动和讲座。南京、上海、深圳等全国主要城市都有我们的身影，金融博物馆、国家会议中心、北京大学等地都摆有我们的展台，其中大部分活动都是免费的，为的就是推广区块链这一概念。

数十场活动下来，我们发现参会的大多是男性，30—40岁居多，金融机构人员、程序员居多。这类人群有一个特点——很少在社交网站上活跃，而且他们在搞懂区块链以后再向其他人讲解时会用到许多技术性名词。这让区块链的推广进展依然缓慢，因为我们每次活动能够影响的也就上千人，但消耗的人力、物力、财力非常巨大，还有部分参会人员是冲着礼品来的。

2016年中旬，直播行业风口四起，流量大量涌入。我们眼前一亮：通过直播推广区块链效果一定很好！而且可以吸引很多年轻人了解区块链！我们马上开始部署，起初我们请出了区块链首席研究员段老师直播讲解区块链，通过各种线上渠道推广，可平均下来每场观看人数不过数百。我们不断反思为什么人家的直播有百万人观看，而我们的只有几百人，还没有人送礼物。这时同事出了一个主意：“你看人家直播都是美女，人长得好看，声音又好听，当然有人看了。”的确很有道理。随即我们又请出了公司里最漂亮的美女同事直播讲解区块链，与此同时加大渠道推广力度，发动群众力量分享朋友圈，可最后也不过是几千人观看。不过值得高兴的是，我们收到的礼物越来越多了，也受到了许多年轻人的关注，但是他们依然不了解什么是区块链，只关心我们的漂亮同事吃没吃饭，有没有男朋友。区块链这一概念的推广，似乎依然很困

难。

持之以恒，我们目前依然在积极尝试各种办法，自媒体、视频、音频、出书等，我们期望区块链这一有可能成为金融底层基础设施的技术，能够像互联网一样走向大众，服务生活。

目前，了解区块链的人大多是大型金融机构雇员或者极客高手，这就导致区块链介绍资料里充满了术语或是技术类名词。而区块链本身又晦涩难懂，这就使一个没有技术背景的人，往往需要用几个月的时间才能搞懂区块链的概念及其历史、基础技术、运行原理和上层应用。

本书的目的就是想将这几个月的时间压缩到一周，甚至几天。

致谢



本书的写作得到了很多热心朋友的帮助，我们不仅获得了来自数字货币、区块链行业内部的支持，很多活跃在互联网、金融领域前沿的资深人士和领导也给予了全方位的帮助。

一项新兴的技术得到社会广泛的认可和应用需要漫长的时间，就像一个个体想要融入集体之中，需要证明自己的价值，这种价值不需要独立于系统之外的自证，而是务必对集体共同利益及生态有正面的推动作用，区块链技术也必须证明这一点。

科普，这是第一个难点。区块链技术是去中心化的分布式账本。单是这句话，就会让很多读者合上这本书了。面对面谈话的时候，当你说

出这句话，可以明显看到对方的眼神飘忽了，能听你滔滔不绝地说上20分钟以上的，就算是感情深的朋友了，一定要好好珍惜。然而这项技术并没有大家想象的那样晦涩难懂、不易理解。

相反，你大可不必研究它的代码构成，你只需要知道，有了这项技术生活体验将发生怎样的变化。这就是我们科普区块链技术的本意。当变化来临时，将头埋在沙子里并不能解决任何问题。令人欣喜的是，在科普和推广区块链技术这条艰难的路上，我们有很多同伴。首先要感谢的是中国金融博物馆理事长王巍老师，他为我们提供了悉心帮助。

王巍老师创立了中国金融博物馆，将其丰富的人生经验和对金融行业的激情注入金融启蒙工作之中，使博物馆立足当下，参与未来。中国金融博物馆成功举办了許多有关区块链技术的线下沙龙活动。本书从创作之初就得到王巍老师的鼓励和支持，他还在百忙之中为本书作序，我们在不胜感激之外深感任重而道远。

融合，这是第二个难点。用新兴的技术解决传统领域的痛点，提升劳动力及资本运转的效率，这是区块链技术发展的动力和使命。而我们常见的“颠覆”“传统行业已死”这类惊悚的标题，大多是为了博人眼球。区块链和互联网相同，都是底层技术，脱离应用层谈技术就是纯粹的“耍流氓”。受益于互联网技术的发展，人们在衣食住行上的体验都大幅提升。区块链技术可以让其中一些体验更加优化。

例如利用数据可追溯、不可篡改的特点，未来人们将在食品溯源及艺术品证伪方面拥有全新的体验。利用智能合约和数据储存的特点，未来人们将在医疗数据的跨平台应用及数据隐私方面取得长足的进步。这些改变与传统行业的初衷并不相悖，如果社会秩序是一个应用的话，区块链技术就相当于一个升级的补丁，你只需要轻点“同意”按钮，体验立刻升级。在舆论和信息不透明机制的影响下，很多传统行业对新兴技术略有一些抗拒和抵触。

然而我们又是幸运的。在推动技术发展的过程中，我们感受到中国传统行业日益开放的态度。传统金融机构、研究机构、各大知名高校不断向我们抛来橄榄枝，要求交流和沟通。这种沟通是相互促进的。我们的老朋友，中信出版集团就一直秉承着用知识改变世界的初衷，不遗余力地帮助我们进行区块链技术的推广工作，在此我们也致以诚致的感谢。此外，夸客金融CEO郭震洲先生、点融网CEO郭宇航先生、蘑菇街高级副总裁杨冰先生，都欣然接受邀请，为本书作序，并在撰书过程中给予了很多鼓励和支持，在此请接受我们的谢意。

世界是变化的，有人恐惧这种变化，有人接受这种变化。保持开放的态度，对新鲜事物给予一定的容纳空间，你的人生总归更有趣一些。新兴技术带来的改变就像暴风雨敲击着你的安乐窝，如果你想假装听不见，那你可以心安地合上本书。

再 见



图书在版编目 (CIP) 数据

图说区块链 / 徐明星, 田颖, 李霁月著. --北京: 中信出版社, 2017.7

ISBN 978-7-5086-7750-7

I. ①图... II. ①徐... ②田... ③李... III. ①电子商务-支付方式-图解 IV. ①F713.361.3-64

中国版本图书馆CIP数据核字 (2017) 第116027号

图说区块链

著者: 徐明星 田颖 李霁月

出版发行: 中信出版集团股份有限公司

(北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029)

电子书排版: 张明霞

中信出版社官网: <http://www.citicpub.com/>

官方微博: <http://weibo.com/citicpub>

更多好书, 尽在中信书院

中信书院: App下载地址<https://book.yunpub.cn/> (中信官方数字阅读平台)

微信号: 中信书院

BLOCKCHAIN REVOLUTION

HOW THE TECHNOLOGY BEHIND BITCOIN IS
CHANGING MONEY, BUSINESS AND THE WORLD

区块链革命

比特币底层技术如何改变货币、商业和世界

[加] 唐塔普斯科特 [加] 亚历克斯·塔普斯科特 著
(Don Tapscott) (Alex Tapscott)

凯尔 孙铭 周沁园 译

“数字经济之父”

继畅销书《维基经济学》之后再出力作
一本真正全景式描述区块链理论及应用的巨著

本书内容源自投资2600多万元的前沿科学研究项目、
100多场与多国政治界、学术界和工商界翘楚人物的对话
前瞻性揭示区块链对银行业、证券业、保险业、会计税收、法律服务业、
文化创意业、物流业、医药卫生业、电力业和制造业等行业产生的深远影响

倾情
推荐

史蒂夫·沃兹尼亚克

苹果电脑共同创始人

马克·安德森

硅谷史德章·霍兰德风险投资公司创始人

克劳斯·施瓦布

世界经济论坛创始人和论坛主席

鲍达民

麦肯锡公司董事兼全球总裁

卢英德

百事公司首席执行官

丹·舒尔曼

Paycom公司首席执行官

肖风

中国万向控股有限公司副董事长

霍学文

北京市金融工作局党组书记、局长

倾情
作序



中信出版集团 · CHINACITICPRESS

区块链革命

——比特币底层技术如何改变货币、商业和世界

[加]唐塔普斯科特 [加]亚力克斯·塔普斯科特 著
凯尔 孙铭 周沁园 译

中信出版社

目录

推荐序一 区块链革命：从《失控》说起

推荐序二 区块链已成为金融科技的底层技术

致谢

第一篇 假如需要变革

第一章 可信的协议

第二章 引导未来：区块链经济七大设计原则

第二篇 转型

第三章 重塑金融服务形象：从赚钱机器变成致富平台

第四章 重新设计公司的架构：核心与边缘

第五章 新商业模式：在区块链上寻找新机会

第六章 万物账本：物理世界的活化

第七章 解决繁荣悖论：区块链的经济包容性

第八章 重建政府和民主

第九章 在区块链上解放文化产业

第三篇 机遇与隐忧

第十章 克服困难：实施过程中的10个挑战

第十一章 下一代的领导者

注释

附录 区块链专业术语表

出版声明

感谢安娜·洛普斯（Ana Lopes）和艾米·威斯曼（Amy Welsman）让这本书成为可能，也感谢她们了解到“这一切都是关于区块链的”。

布赖恩·福德

麻省理工学院媒体实验室数字货币计划

这是一本必须读的书。你将会深刻地理解到为何区块链技术正快速成为自互联网诞生以来最重要的新技术。

尤查·本科勒

哈佛大学法学院企业法律研究系讲座教授

区块链是一股强劲的技术浪潮，而这次塔普斯科特父子联手进行探索，再一次站在了时代的前沿——这就如他们在以往的每个新兴的技术浪潮中做所做的事情一样。这真是一场难得的经历。

马克·安德森

网景及硅谷安德森·霍洛维茨风险投资公司创始人

区块链是计算机科学史上最基础的发明之一，要理解它的深远意义就要好好阅读《区块链革命》这本书。

史蒂夫·沃兹尼亚克

苹果电脑共同创始人

《区块链革命》是一本多么具有震撼力的好书！内容深刻！让人耳目一新！此书让我感觉人类又到了一个技术、经济和社会历史又将被突破的紧要关头。

伊藤穰一

麻省理工学院媒体实验室主管

区块链在信任中发挥的作用正犹如互联网在信息中发挥的作用。就如早期的互联网一样，区块链有潜力革新一切。读一下这本书你就会明白了。

鲍达民

麦肯锡公司董事长兼全球总裁

《区块链革命》的观点研究充分，文字优美，阐述了价值互联网将如何改变我们的生活，是当前变革时代不可或缺的图书。

克劳斯·施瓦布

世界经济论坛创始人和论坛主席

图书市场偶尔会有改变全球话题的书蹦出来，《区块链革命》很可能就是当中的一本！区块链是第四代工业革命的动力之源。作者用通俗易懂的语言向世人解释我们为什么要抓住这个机遇以及如何才能抓住机遇，避免陷入危险境地。

纳塔拉詹·钱德拉塞克兰

塔塔咨询服务公司首席执行官及总经理

这本书很好地说明了区块链在提高透明性及保护隐私权方面的能力。用作者的话说，就是物联网需要一个为万物而设的账本。

丹·舒尔曼

Paypal公司首席执行官

世上每个思维缜密的人都在试图明白区块链这一革命性的技术及其将如何改变世界的面貌。唐塔普斯科特团队超前一步，创作出了众人期

待的《区块链革命》。

戴夫·麦凯

加拿大皇家银行主席及首席执行官

在这个通往金融世界前沿领域的非凡旅程中，作者阐述了与区块链相关的现象，并有力地说明了为何我们需要进一步了解区块链技术的力量及其潜力。

本杰明·罗斯基

美国纽约州金融服务部前主任、罗斯基集团首席执行官

唐和亚历克斯为那些尝试驾驭这个全新的、有着发展前景的前沿机会的人写下了这本有着决定性意义的指导手册。

史蒂夫·卢克佐

希捷技术主席及首席执行官

难以置信，真的是难以置信！塔普斯科特父子细致入微地解释了区块链在这个中心化程度日渐强化的世界中作为一种具备包容性的模式的意义。这非常厉害！

布赖恩·费瑟斯通豪

奥美公共关系国际集团主席及首席执行官

作者发现了一个意义深远的技术运动并将其与信任这种最深刻的人类需求连接起来。这本书的研究非常细致，行文也十分引人入胜。每一个认真的商务人士和政策制定者需要阅读《区块链革命》这本书。

卢英德

百事公司首席执行官

《区块链革命》简洁明了阐释区块链技术将来如何深远影响我们处理信任、安全和隐私问题的方式方法。

保罗·波尔曼

联合利华首席执行官

《区块链革命》这本书对这个有潜力重构全球经济的技术所提供的见解对读者来说很有吸引力和鼓舞力。这是一份难能可贵的礼物！这是一本多么好的书！

埃里克·布林约尔松

麻省理工学院教授、《第二个机器时代》的共同作者

如果你是在商界或政府工作，你需要了解这场区块链革命。除了塔普斯科特两父子外，没有人在这个题材上写过一本研究得如此细致、如此引人入胜的书籍了。

泰勒·文克莱沃斯

格米尼与文克莱沃斯资本联合创始人

《区块链革命》很好地记录并阐释了去中心化的、不依赖于信任关系的金钱所构成的美好新世界。

弗兰克·布朗

泛大西洋资本集团总经理及首席运营官

《区块链革命》预告了一波即将来临的技术进步的浪潮——这股浪潮才刚开始。

比尔·麦克德莫特

企业资源管理软件方案提供商SAP SE首席执行官

世界上很少有唐塔普斯科特这样能够促使我们环顾四周的领导者。他和他的儿子亚历克斯通过《区块链革命》教育了我们、挑战了我们，并向我们展示出一种对未来进行思考的全新方式。

赫尔南多·德·索托

秘鲁自由和民主学院经济学家及主席

这是一部杰出的作品。它优雅地展示出了区块链技术应对当前世界所面临的迫切挑战的潜力。

吉姆·布雷耶

布雷耶资本首席执行官

《区块链革命》就如数字货币世界的一本地图集，巧妙地解释了当前的形势，同时为我们通向一个更公平、更高效及更四通八达的全球金融系统指出了一条前进的道路。

埃里克·施皮格尔

西门子美国分公司主席及首席执行官

过去要花一代人的时间才能实现的技术变革，现在就像在眨眼之间就发生了，而没有人能比塔普斯科特父子更好地讲述这个故事了。

布莱思·马斯特斯

数字资产控股首席执行官

如果有什么需要启蒙的题材，那就是区块链了。塔普斯科特父子一起深入地实现了这个题材的启蒙，并在这个过程中向所有人展示出了这个题材的兴奋点、潜力及重要性。

蒂姆·德雷珀

德雷珀事务所、德丰杰创始人

这是一本有着奥威尔的《1984》那样的预见性及伊隆·马斯克那样的眼界的书。你要读一下，否则就会被淘汰了。

杰里·布里托

比特币政策智库Coin Center董事长

《区块链革命》是通往这个能改变世界的技术的不可缺少及决定性的指南。

弗兰克·德索萨

高知特科技首席执行官

信任的中心点将要扩散开来了！这本书详细叙述了一个去中心化的信任系统的革命性潜力。

佩里安·博林

数字贸易商会创始人及主席

区块链技术有潜力实现产业、金融及政府的变革，任何对未来的财

富及人类社会有兴趣的人都应该读一下这本书。

雷·莱恩

巨点投资管理合伙人、凯鹏华盈荣誉合伙人

当划时代的技术改变我们所处的世界时，我们真的很幸运有唐塔普斯科特这样的（现在还有他的儿子亚历克斯）这样精于描绘蓝图的人来为我们解释未来的方向。

亚历克·罗斯

《未来产业》作者

作者深入浅出地解构了区块链的潜力和可能面临的障碍。《区块链革命》让读者有机会对未来的世界先睹为快。

道格拉斯·洛西克夫

《现在的冲击》与《对谷歌公共汽车投掷石块》的作者

比特币的底层技术会如何释放出一个为分布式繁荣而设的数字经济的真正潜力？这本书给出了一个不可缺少的、及时的分析。

詹姆斯·里卡兹

《货币战争》及《金钱之死》的作者

《区块链革命》将历史、技术和社会学的元素精妙地结合起来，涵盖了区块链协议的所有角度。区块链协议在以后可能会被证明能与印刷术的发明的重要性相提并论。

丹·庞蒂弗拉克特

《目标效应》作者、研科公司（TELUS）首席战略家

《区块链革命》是为下一个数字时代而书写的一份有启发性的、极其重要的纲领。

安德烈亚斯·安东诺普洛斯

《掌握比特币》的作者

这是一本在这个互联网后最令人兴奋的新技术的话题上研究得最好、最细致及最有洞察力的书。它有着无与伦比的清晰程度、令人惊讶的广度及深入见解。

沃尔特·艾萨克森

《乔布斯传》作者

互联网最缺乏的元素就是“信用协议”，以便确定每项交易是被核准且真实有效，而区块链技术可能为解决此问题提供基础。区块链确实是重大变革性，而《区块链革命》用浅显易懂的语言阐述了区块链是变革性的原因。

克莱顿·克里斯坦森

《创新者的窘境》作者

唐普斯科特父子撰写的《区块链革命》客观真实，并非耸人听闻，该书告诉人们在下一波由技术驱动的大变革中该如何滋润地生存下来。

推荐序一

区块链革命：从《失控》说起

《失控：全人类的最终命运和结局》是著名作家凯文·凯利写于20世纪90年代初，关于自然万物、人类社会和科学技术如何进化的著作。彼时，互联网标准协议在经过长达近三十年的实验和争议后，刚刚被确定为网络通讯协议（TCP/IP）分层结构。但凯文·凯利在那时候就几乎预言到了今天互联网世界所发生的一切：移动互联网、云计算、大数据等等。

微信之父张晓龙对《失控》推崇备至。想必《失控》这本书对他创造微信产生过巨大影响。该书在出版十几年后突然在中国红火，一是因为张晓龙的推荐；二是在当今重读这本书，不仅可以帮助我们理清互联网世界的发展历程，还仍然可以指引我们认清互联网世界的未来趋势。

甚至我们也可以从《失控》中看到他对区块链技术出现的预言。《失控》这本书的主题词基本可以概括为三句话九个字：分布式、去中心、自组织。这是他总结的独具特色的生物学进化论的中心逻辑框架。生物学进化论是相对于工业革命的机械学进化论而言的。大家都知道，工业革命的特色之一就是强调结构、标准和控制。而凯文·凯利的观点从书名《失控》就能一目了然：从控制到失控；从边缘到中心；从他治到自治。

在《失控》书中，凯文·凯利专门解释了分布式网络的特性：没有强制性的中心控制；次级单位具有自治的性质；次级单位之间彼此高度连接；点对点间的影响通过网络形成了非线性因果关系。我们从中可以领会到的就是弱控制、分中心、自治机制、网络架构和耦合连接等等与

工业社会完全不同的信息社会时代的新型的社会结构、商业模式、人际关系。这其实就是区块链技术的全部精要！区块链正是基于分布式系统集成多项成熟技术而成的。区块链的点对点价值传输、分布式数据库、分布式账本、智能合约和可编程数字货币就是凯文·凯利在《失控》一书中探讨的分布式网络在工程技术层面的具体实现。

区块链革命的逻辑起点就在于此！因为只有分布式网络在工程技术层面能够得以实现，凯文·凯利所倡导的基于生物逻辑，生于信息社会的分布式、去中心、自组织的新进化论才能产生类似摩尔定律那样的指数级影响力。

利用为本书写推荐序的机会，先睹为快，学到很多新东西，得到很多新启发。我认为区块链要对现实世界产生革命性影响，有几个问题必须澄清：

（一）区块链的核心是分布式而不是去中心。根据凯文·凯利的定义，分布式系统“没有强制性的中心控制”，这里的意思明显说的是分布式系统弱化了中心控制，而不是消灭了中心控制。区块链是弱中心化的、分中心化的。在凯文·凯利的眼里，去中心是一个过程而不是一个结果，一个新的具有更高效率和更低成本的新生事物，必定会将陈旧僵化的旧中心取而代之！这才是进化论者眼里的人间正道！进一步而言，公平与效率这两者永远是对立统一的矛盾体，区块链也许能够使得公平和效率更加接近最优平衡，但至少目前的技术仍然看不到消弭这两者间隙的可能性。区块链希望在分布式账本上依靠去中心的共识算法来保持数据的高度一致性，这就无法照顾到效率。这个公平与效率的宿命，基本上在区块链上还是没能完全打破。

（二）区块链是分布式账本，但分布式账本不一定是区块链。人类社会有史以来的任何具有革命性的发明创造，基本都是由具有强烈价值观的人搞出来的。没有强烈的价值观的驱使，人们就不可能会去颠覆旧世界。毋庸置疑，区块链技术确实是由一群具有强烈无政府主义价值观

的技术极客们创造出来的。人类社会几千年来无政府主义者的任何尝试都以失败告终，这一次，技术极客们希望利用区块链技术，在网络空间、虚拟社会里建立一个去中心化的自治社区。比特币区块链作为一个小范围的实验，在过去七年的时间里证明了分布式网络确实有不少值得借鉴的技术优势。金融机构试图对比特币区块链去伪存真，隐恶扬善。于是，他们对像比特币区块链那样的公共区块链进行了一番改造，去掉了原生数字货币、允许多中心机构的多节点的弱控制、改进了共识算法并加入了更强的隐私保护加密算法。为了强调与去中心化的公共区块链的区别，这个改造过的区块链，被刻意命名为分布式账本，而不再称为区块链了。

（三）区块链在工程技术层面还不够成熟，离金融行业大面积应用还需要数年时间。区块链上一直有两拨人，在不同的方向做着不同的事。一拨人专注于挖矿、炒币甚至发行自己的数字货币筹资，业界俗称“币圈”；另一拨人专注于区块链技术的研发、应用，甚至从区块链底层协议编程开始做起，业界俗称“链圈”。区块链技术目前的成熟程度，对于“币圈”来说，已经足够满足他们的需求，因此他们对区块链技术的进一步发展并不关心。但是对于积极探讨区块链在各行各业应用的“链圈”来说，区块链技术目前还存在不少技术瓶颈，妨碍了各行各业的区块链+。比如现有共识算法如果不优化，按照比特币区块链每秒七笔交易的速度，金融交易层面就无法使用区块链技术；比如公共区块链帐户余额是向全网公开的，而银行必不能接受客户帐户余额向全网公开的做法，这就需要新的隐私保护算法，而这方面的加密算法还没有一个达到生产级别应用的水平；再比如区块链的可编程性是各国央行发行数字货币的最大吸引力，也是金融行业对区块链技术的最大期许。但TheDAO事件^[1]提醒我们，应该有一个能对智能合约进行事先检验的科学方法，但这方面最先进的技术如形式化验证，目前还处于理论研究阶段。看热闹可以，入戏太深就容易从先驱变成先烈！

（四）“代码即法律”只是乌托邦理想，智能合约也只是帮助执行双

方约定的计算机程序而已。智能合约既不是人工智能，也不是法律合同，只是帮助执行双方约定条件的一段计算机程序。确实，一旦把双方约定写入智能合约，计算机程序在技术上可以保证做到不可反悔、不可篡改及按照约定自动执行，但代码即法律就像网络完全自治一样，基本不可能见容于现实社会。缔结、编制智能合约的依据可能大部分还是要来源于现实世界的法律体制，比如产权的登记和确认；网络世界里发生的纠纷，最终还会需要一个第三方独立机构来提供最后的司法仲裁和救济；区块链的可编程性确实可能带来价值交换的点对点化和金融交易的自动化、智能化，但这只是对法律体系和金融体系从技术上带来了革新机会，而不是改朝换代般的革命。

（五）比数字货币范围更大、价值更大的是数字资产。数字资产是指在区块链上登记、发行、交易的资产；它往往以数字代币（token）的方式记录在分布式账本上，coin是它的货币单位；我们知道英语中表示货币的单词有三个：currency、money、coin，currency更多的是央行眼里的货币，当我们谈到利率、汇率和流动性时，我们指的是“currency”；当金融机构谈到资金时，我们谈的是“money”；未来，当我们谈到数字资产时，我们谈的是“coin”，“coin”在链圈的眼里，实际上就是数字资产代币。人类社会正在进行一场数字化大迁徙，我们正在网络世界、虚拟空间里建立一个数字化新世界，这个新世界可能蕴藏着比物理世界、现实社会更大的财富宝藏。互联网、区块链、增强现实技术（AR）、虚拟现实技术（VR）、人工智能（AI）等各种各样的新技术都是人类驶向数字世界的帆船。我们一定要争做数字世界的新移民，千万不要做了物理世界的旧遗民！值得提醒的是：大家不要拘泥于数字货币这个小圈子，而要投身于区块链在各行各业的应用研究中。有大视野才有大事业！

《区块链革命》，是我目前见到的对区块链技术介绍、剖析和定位得最精准的一本书。其大局观颇具胸襟，于细微处洞若观火。开卷，可以扩人眼界、指人方向；掩卷，可以令人遐想、引人深思！

万向区块链实验室很高兴再一次与中信出版社合作，组织翻译出版这部代表区块链行业最高水平的著作，以飨读者，以利行业。期待与大家共同推动中国的区块链事业朝着正确的方向前进！

肖风

中国万向控股有限公司副董事长

2016年9月1日

[\[1\]](#) 北京时间2016年6月17日，黑客利用TheDAO（区块链业界最大的众筹项目）编写的智能合约中的重大缺陷展开网络攻击，造成300多万以太币资产被分离出TheDAO资产池（被攻击前拥有1亿美元左右资产）的财产损失事件。

推荐序二

区块链已成为金融科技的底层技术

金融=制度+技术+信息。

在互联网时代，在金融技术发展日新月异的时代，在金融边缘创新不断向中心地带侵蚀并不断融入其中的新金融时代，在传统金融不断信息化、网络化、数字化时代，金融已经远远突破了资金融通的传统内涵，金融技术已经将金融信息与金融科技高度融合，技术成为驱动金融发展的底层力量，成为一个大趋势。在互联网时代，驱动金融发展的金融科技已经由移动互联网、大数据、云计算等应用层面，进一步转向了区块链等底层技术创新。区块链已经成为金融科技的底层技术。

我的朋友肖风博士，以极大的努力推动着区块链技术在金融领域的应用，以极高的诚意促进着区块链领域知识普及与研究交流，以种子基金形式投资了很多国内外领先的区块链金融企业。我从他身上和他投资的企业，不断看到他在这个领域的全面进步与执着探索。他牵头创建的中国分布式总账基础协议联盟（ChinaLedger）将在中国区块链领域起到里程碑式的基础性作用。他是区块链金融的布道者、研究者、投资者和实践者。

借《区块链革命》一书出版之际，我谈一点我读书之后的认识，作为此书作者的一种敬意。

一、区块链技术的内涵与实质

区块链（Blockchain）是一个由不同节点共同参与的分布式数据库系统，是开放式的账簿系统（ledger）；它是由一串按照密码学方法产生的数据块或数据包组成，即区块（block），对每一个区块数据信息都自动加盖时间戳，从而计算出一个数据加密数值，即哈希值（hash）。每一个区块都包含上一个区块的哈希值，从创始区块（genesis block）开始链接（chain）到当前区域，从而形成区块链。

区块链技术的实质是在信息不对称的情况下，无需相互担保信任或第三方（所谓的“中心”）核发信用证书，采用基于互联网大数据的加密算法创设的节点普遍通过即为成立的节点信任机制。任何机构和个人都可以作为节点参与创设信任机制，而且创设的区块必须在全网公示，任何节点参与人都看得见。节点越多，要求的算力就越强，只有超过51%的节点都通过，才能确立一个新区块成立，即获得认可；同时，要想篡改或造假，也需要掌控超过51%的节点，才可以修改。理论上，当区块链的节点达到足够数量时，这种大众广泛参与的信任创设机制，就可以无需“中心”授权即可形成信任、达成和约、确立交易、自动公示、共同监督。

市场经济活动中存在众多信息中介和信用中介，原因就在于信息不对称导致交易双方无法建立有效的信用机制（“拜占庭将军问题”）。区块链技术为解决这一问题提供全新的思路。移动互联网、大数据、云计算是区块链技术的基础设施，算法信任是关键机制，加密算法是技术基础。比特币的创始人中本聪对区块链技术应用做出了奠基性的贡献。

二、区块链技术将广泛应用于金融领域

金融领域是区块链技术的重要应用领域。区块链技术将是互联网金融乃至整个金融业的关键底层基础设施（底层物质技术基础）。区块链技术可以低成本地解决金融活动的信任难题，并且将金融信任由双边互

信或建立中央信任机制演化为多边共信、社会共信，以“共信力”寻求解决“公信力”问题的途径。由于区块链技术的加密算法特性，未来金融业会发展进入算法金融时代。

比特币是区块链技术应用的一个典型案例，虽然它不能当作法定货币，但是却为数字货币时代的到来和区块链技术广泛应用于解决金融、经济和社会问题，提供了底层技术基础。国内外金融界正在探索这一未来金融底层技术的技术制高点，发达经济体的大金融机构创设的国际银行区块链联盟组织(R3)在加紧研究区块链技术的金融应用，德勤(Deloitte)已经将这种技术应用于企业审计，纳斯达克市场尝试利用区块链技术发行证券。中国的金融界也在关注这一趋势，北京已经组建多个区块链技术联盟，成立区块链技术金融应用的金融科技公司，专门设立互联网金融安全产业园，集中推进金融科技产业发展。

作为新金融的底层技术架构，它具有很强的战略意义。继互联网之后，区块链技术再次重塑全球金融业的基础框架，加速金融创新与产品迭代速度，极大提高金融运行效率，重塑信用传递交换机制。在未来金融科技探索上，中国金融业应该加强研究、开发、实践和应用，积极组建国际区块链联盟，加强区块链金融国际交流合作，参与创立区块链技术标准，推动金融科技的顶层设计，争取国际金融战略制高点，提升我国金融核心竞争力，让金融更好为实体经济服务。

三、互联网金融将进入到“区块链+”时代

区块链作为金融科技的底层技术架构，必然在很多方面重塑金融业态，无论是传统金融服务，还是个人网贷（P2P）、众筹等互联网金融创新，抑或在强化金融监管、防范金融风险、打击非法集资等领域，区块链技术都有非常广阔的应用前景，互联网金融正在进入“区块链+”时代。

（一）区块链+支付（国际结算）。支付是金融市场最重要的基础设施，区块链技术最先革新领域就是支付清算。以瑞波实验室

（Ripple）为例，尽管他还有需要完善和改进之处，但是它是目前一个相对成熟的区块链支付服务。它是一种基于互联网的开源支付协议，可以实现去中心化支付与清算功能。在Ripple系统里，所有的货币均可自由兑换，不仅包括各国的法币，而且包括虚拟货币。Ripple系统里的货币兑换和交易的效率更高、速度更快，且交易费用几乎为零，交易确认在几秒钟内完成，没有异地和跨行费用。现有的国际货币兑换模式主要通过加入环球银行金融电信协会（SWFIT）的银行间清算和结算，而Ripple是一个开源的点对点网络，构建了一套完全不同的账户体系。它实质上是一个可共享的开源数据库，可以快速、廉价并安全地将资金转账到任何人或任何机构在Ripple系统中的账户，没有任何人或任何机构能控制Ripple网络。这是分布式的账簿体系，实际上体现了区块链技术的核心思想，未来有广阔的发展前景。

（二）区块链+征信。征信市场是一个巨大的蓝海市场。传统征信市场面临信息孤岛的障碍，如何共享数据成分发掘数据蕴藏的价值，传统技术架构难以解决这个问题。区块链技术，为征信难题提供了一种全新的思路。首先，提高征信的公信力，全网征信信息无法被篡改。其次，显著降低征信成本，提供多维度的精准大数据。最后，区块链技术有可能打破数据孤岛的难题，数据主体通过某种交易机制，通过区块链交换数据信息。实现这种高效的征信模式，还有业务场景、风险管理、行业标准、安全合规等一系列问题要解决。

（三）区块链+交易所。交易所是集中交易某种有形或者无形的市场，区块链技术将在各式各样的产权交易得到广泛应用。区块链的去中心化、开放性、共享性、匿名性、不可篡改性等特征，可以显著提升登记、发行、交易、转让、交割清算效率，也可以保障信息安全与个人隐私。纳斯达克市场和澳洲交易所在区块链技术应用上走在了前列。2015年末，纳斯达克——全球最大的证券交易所之一，首次使用了区块

链技术交易平台，完成和记录私人证券交易。澳洲交易所利用区块链技术与银行账户连接，买卖股票后资金可以迅速到账。现在的应用还只是在证券发行和资金清算环节，未来区块链技术在各种产权交易中必然会发挥更大的作用，甚至成为很多领域的主要交易系统。

（四）区块链+数字货币。区块链技术最早应用于比特币，很多人投资比特币、交易比特币，也有商业活动、经营场所接受比特币支付。但是，比特币天然不是法定货币，比特币为法定货币（含纸币）进入电子货币后的数字货币时代，奠定了技术基础和应用示范。中国人民银行已经开展数字货币研究，很多国家中央银行也积极研究数字货币。法定数字货币的应用，必须建立在全网信息记录、信用实时计算、全民网上诚信、底层技术安全、货币法定授权、算法不可破解等技术基础上。数字货币会提升全民的自我信用管理水平，提升共享经济水平，提升金融服务实体经济的水平，也将促进互联网金融的健康规范发展。

当前区块链技术仍然处于蓬勃发展的初级阶段，在鼓励支持区块链技术创新的同时，我们更要防范潜在的金融风险，避免其成为非法金融活动的来源，引导其走向良性健康、规范合法的轨道上。特别是吸取网贷行业的经验教训，避免监管真空，高度警惕打着“区块链技术”旗号从事非法集资、金融诈骗等非法金融活动的现象，守住不发生区域性金融风险的底线。

区块链技术的作为未来金融业的底层技术，已经得到了各国央行和金融机构的广泛认同，正在研究通过区块链技术深化金融改革、提升金融供给、促进金融创新、增强金融信用、防范金融风险，相信区块链技术，这一金融底层技术，将在金融领域乃至经济、社会领域，得到广泛的应用。

是为序。

霍学文

北京市金融工作局党组书记、局长
2016年9月1日

致谢

这本书源自两个不同的头脑及人生轨迹的碰撞。唐塔普斯科特一直在加拿大多伦多大学罗特曼管理学院带领一个名为全球解决方案网络的项目。这个项目当时在调查用于解决全球问题和治理机制的新型网络化模式。他研究了互联网是如何被一个由多个利益相关方组成的生态系统所治理的，然后开始对数字货币及其治理机制产生了兴趣。同时，亚历克斯是加拿大投资银行集团的一名管理人员。他在2013年注意到了比特币及区块链公司早期的持续增长的热度，并开始带领他的公司朝着这个领域发展。在2014年早期，在一场两父子去蒙特朗布朗的滑雪旅程中，我们在餐桌上展开了对这个题材进行协作的头脑风暴，而亚历克斯同意了带领一个在数字货币治理方面的研究项目，最终体现在了他的一篇题为《一种比特币的治理网络》的白皮书中。随着我们对这个题材研究的日渐深入，我们越来越意识到这可能是下一个能带来剧变的事物。

与此同时，我们的演讲者管理机构Leigh Bureau经纪人韦斯·内夫（Wes Neff），与唐有业务往来的企鹅出版集团的Portfolio出版社的阿德里安·扎克海姆（Adrian Zackheim）一起，开始鼓励唐构思一本新书的题材。这个出版社的经典出版物有《维基经济学》以及《宏观维基经济学》。当亚历克斯的论文开始在这个领域被视为是前沿思想的时候，唐让亚历克斯成为他的共同作者。另外还要感谢阿德里安，给出了一个我们无法拒绝的提议，而这本书从来没有经历过一个竞卖的环节（通常情况下是要经过这个环节的）。

之后，我们就做出了一个在事后看来很聪明的选择。我们找到了所知道的最好的书籍编辑柯尔丝滕·桑德伯格（Kirsten Sandberg），她之前在哈佛商学院出版社工作过。我们让她对我们的成书清样进行编辑。

她的工作令人十分满意，鉴于我们的合作可谓是毫不费力的，因此我们让她成为这本书的研究团队的一名全职成员。柯尔丝滕跟随着我们参与了超过100场采访，并在我们试图理解所面临的众多问题时进行实时协作，然后一起构想将这些非凡的发展成果解释给非技术听众的简洁陈述内容。她帮助我们将这些故事带到了眼前。在这个意义上，她是我们这本书的一位共同作者，若没有她的参与，这本书也无法面世（至少也不会以目前的这个极其详尽的版本面世）。我们对这样的贡献，以及对在这个过程中出现的灵感碰撞及有趣的小插曲，表示衷心的感谢。

我们也衷心感谢下面的人，他们慷慨地向我们分享了他们的时间和见解，如果没有他们这本书也不可能完成。下面的名单以阿拉伯字母为序：

杰里米·阿莱尔Jeremy Allaire

跨境支付公司Circle创始人、主席、首席执行官

马克·安德森Marc Andreessen

著名风投机构Andreessen Horowitz的联合创始人

加文·安德烈森Gavin Andresen

比特币基金会首席科学家

迪诺·马克·安格里蒂斯Dino Mark Angaritis

基于区块链的全球各种有价资产交易平台智能钱包公司（SmartWallet）的首席执行官

安德烈亚斯·安东诺普洛斯Andreas Antonopoulos

《掌握比特币》作者

费德里科·阿思特Federico Ast

大众司法系统网站CrowdJury

苏珊·阿西Susan Athey

斯坦福商学院技术经济教授

亚当·巴克Adam Back

区块链公司Blockstream联合创始人及董事长

比尔·巴希特Bill Barhydt

去中心化汇兑公司Abra首席执行官

克里斯托弗·巴维兹Christopher Bavitz

哈佛法学院网络法律诊所总经理

杰夫·比蒂Geoff Beattie

风投机构Relay Ventures主席

史蒂夫·博勒加德Steve Beauregard

比特币支付网关GoCoin首席执行官和创始人

马里亚诺·贝林基Mariano Belinky

投资机构Santander InnoVentures管理合伙人

尤查·本科勒Yochai Benkler

哈佛法学院企业法律研究系讲座教授

杰克·本森Jake Benson

数字货币税务处理软件公司LibraTax的首席执行官和创始人

蒂姆·伯纳斯-李Tim Berners-Lee

万维网发明者

道格·布莱克Doug Black

加拿大政府参议院的参议员

佩里安·博林Perianne Boring

数字贸易商会（Chamber of Digital Commerce）创始人及主席

戴维·布雷David Bray

2015艾森豪研究项目研究员及哈佛大学驻企高管

杰里·布里托Jerry Brito

比特币政策智库Coin Center执行董事

保罗·布罗迪Paul Brody

安永会计师事务所技术组美洲战略领导者(之前任职于IBM的物联网部门)

理查德·甘道·布朗Richard G. Brown

国际银行区块链联盟R3 CEV首席技术官(曾任IBM产业创新及商业发展部门的前执行架构师)

维塔利克·布特因Vitalik Buterin

以太坊创始人

帕特里克·伯恩Patrick Byrne

在线零售商Overstock首席执行官

布鲁斯·卡恩Bruce Cahan

斯坦福大学工程学院访问学者、斯坦福可持续银行业计划成员

詹姆斯·卡莱尔James Carlyle

R3 CEV银行联盟首席工程师及总经理

尼古拉斯·卡里Nicolas Cary

区块链公司Blockchain Ltd. 联合创始人

托尼·莱恩·卡瑟利Toni Lane Casserly

比特币媒体网站CoinTelegraph首席执行官

克里斯琴·卡塔利尼Christian Catalini

麻省理工大学斯隆管理学院助理教授

安·卡沃基安Ann Cavoukian

瑞尔森大学隐私和大数据学院执行主任

文特·瑟夫Vint Cerf

互联网的共同创始人，谷歌首席互联网传道者

陈斌Ben Chan

比特币安全平台BitGO高级软件工程师

罗宾·蔡斯Robin Chase

Zipcar（服务聚合公司）联合创始人及前任首席执行官

法迪·查哈迪Fadi Chehadi

互联网名称与数字地址分配机构（ICANN）首席执行官

康斯坦丝·蔡Constance Choi

咨询机构Seven Advisory负责人

约翰·H·克利平格John H. Clippinger

ID3（创新与数据驱动设计研究所）首席执行官，麻省理工学院媒体实验室研究科学家

布拉姆·科恩Bram Cohen

分布式文件分享软件BitTorrent创始人

埃米·科特斯Amy Cortese

媒体《投资本土化》（Locavest）创始人、记者

肯尼迪·考维尔J.F.Courville

加拿大皇家银行财富管理部门首席运营官

帕特里克·迪根Patrick Deegan

身份识别初创公司个人黑盒子（Personal BlackBox）首席技术官

普里马韦里·德菲利皮Primavera De Filippi

法国国家科学研究中心（CNRS）终生研究员及哈佛法学院伯克曼互联网与社会中心高级助理

赫尔南多·德·索托Hernando de Soto

秘鲁自由民主学院经济学家及主席

佩罗内蒂·德佩涅Peronet Despeignes

预测市场平台Augur特殊运作业务

雅各·迪内尔特Jacob Dieneltit

Bit交易所及公证通区块链架构师及首席财务官

乔尔·迪茨Joel Dietz

区块链公司Swarm Corp

海伦·迪斯尼Helen Disney

比特币基金会前任成员

亚当·德雷珀Adam Draper

风投机构Boost VC首席执行官及创始人

蒂莫西·库克·德雷珀 Timothy Cook Draper

风投资本家及德丰杰（DFJ）创始人

安德鲁·达德利 Andrew Dudley

监测网络地球观察创始人及首席执行官

约书亚·费尔菲尔德 Joshua Fairfield

华盛顿与李大学（Washington and Lee University）法学教授

格兰特·丰多 Grant Fondo

高赢律师事务所(Goodwin Procter LLP) 隐私与数据安全业务、证券诉讼与白领辩护组合伙人

布赖恩·福德 Brian Forde

白宫前高级顾问；麻省理工学院媒体实验室数字货币计划主任

迈克·高尔特 Mike Gault

安全技术公司Guardtime的首席执行官

乔治·吉尔德 George Gilder

吉尔德科技基金（Gilder Technology Fund）创始人及合伙人

杰夫·戈登 Geoff Gordon

加拿大比特币服务公司Vogogo首席执行官

维纳伊·古普塔Vinay Gupta

以太坊（Ethereum）发布协调员

詹姆斯·哈泽德James Hazard

法务自动化公司Common Accord创始人

伊摩琴·希普Imogen Heap

获得格莱美奖的音乐家及作曲家

迈克·赫恩Mike Hearn

谷歌前工程师，创建了比特币公司Vinumeris公司及去中心化众包灯塔项目

奥斯汀·希尔Austin Hill

区块链公司Blockstream联合创始人及首席推广者

托马斯·亨德里克·伊尔韦斯Toomas Hendrik Ilves

爱沙尼亚总统

伊藤穰一Joichi Ito

麻省理工学院媒体实验室主任

埃里克·詹宁斯Eric Jennings

物联网公司Filament的联合创始人及首席执行官

伊莎贝拉·卡明斯卡Izabella Kaminska

《金融时报》的金融记者

保罗·肯普-罗伯逊Paul Kemp-Robertson

营销机构Contagious Communications联合创始人及编辑主任

安德鲁·基斯Andrew Keys

以太坊生态圈区块链公司共识系统公司

伊丝·金Joyce Kim

恒星发展基金会执行董事

彼得·柯尔比Peter Kirby

公证通（Factom）首席执行官及联合创始人

乔伊·克鲁格Joey Krug

预测市场平台Augur核心开发者

哈洛克·库林Haluk Kulin

个人黑盒子首席执行官

克里斯·拉森Chris Larsen

瑞波实验室（Ripple Labs）首席执行官

本杰明·罗斯基Benjamin Lawsky

纽约州金融服务部前主任，罗斯基集团首席执行官

李启威Charlie Lee

莱特币（Litecoin）前任工程主管、创始人及首席技术官

马修·莱博维茨Matthew Leibowitz

投资机构Plaza Ventures合伙人

文尼·林厄姆Vinny Lingham

礼品卡公司Gyft首席执行官

利亚诺斯Juan Llanos

数字资产管理公司Bitreserve.org战略伙伴及首席透明官

约瑟夫·卢宾Joseph Lubin

以太坊生态圈区块链公司Consensus Systems首席执行官

亚当·鲁德温Adam Ludwin

区块链技术公司Chain.com的创始人

克里斯汀·伦德奎斯特Christian Lundkvist

任职于基于以太坊的三式记账法初创公司Balance3

戴夫·麦凯Dave McKay

加拿大皇家银行主席及首席执行官

扬娜·麦克马纳斯Janna McManus

比特币矿机公司BitFury全球公关总监

米基·麦克马纳斯Mickey McManus

玛雅研究所

杰西·麦克沃特斯Jesse McWaters

世界经济论坛的金融创新专家

布莱思·马斯特斯Blythe Masters

数字资产控股（Digital Asset Holdings）首席执行官

阿利斯泰尔·米切尔Alistair Mitchell

投资机构Generation Ventures管理合伙人

卡洛斯·莫雷拉Carlos Moreira

密码学安全公司WiSeKey的创始人、主席及首席执行官

汤姆·莫宁尼Tom Mornini

会计行业初创公司Subledger创始人及客户需求专家

伊桑·纳德尔曼Ethan Nadelmann

药物政策联盟（Drug Policy Alliance）执行董事

亚当·南吉Adam Nanjee

技术公司MaRS金融科技集群负责人

丹尼尔·奈斯Daniel Neis

支付业务公司KOINA首席执行官及联合创始人

凯利·奥尔森Kelly Olson

英特尔公司新业务行动

史蒂夫·奥莫亨德罗Steve Omohundro

智库机构Self-Aware Systems主席

吉姆·奥兰多Jim Orlando

加拿大安大略省雇员退休金计划（OMERS Ventures）总经理

劳伦斯·奥尔西尼Lawrence Orsini

能源服务公司罗山能源（LO3 Energy）联合创始人及负责人

保罗·帕奇菲科Paul Pacifico

艺术工作者联盟首席执行官

乔斯·帕格里尔Jose Pagliery

美国有线电视新闻网络财经网记者

斯蒂芬·佩尔Stephen Pair

比特币支付公司BitPay Inc.的联合创始人及首席执行官

维克拉姆·潘迪特Vikram Pandit

花旗银行前首席执行官，任职于投资机构Portland Square Capital，比特币交易所Coinbase的投资者

杰克·彼得森Jack Peterson

预测市场平台Augur核心开发者

埃里克·皮斯奇尼Eric Piscini

德勤银行业与技术主管

考西克·拉戈帕尔Kausik Rajgopal

麦肯锡的硅谷办公室负责人

苏雷什·拉马穆尔蒂Suresh Ramamurthi

堪萨斯州的一家小型银行CBW Bank的主席及首席技术官

珊妮·雷Sunny Ray

印度比特币公司Unocoin.com首席执行官

卡特琳娜·林迪Caterina Rindi

区块链公司Swarm Corp社区管理员

爱德华多·罗布尔斯·埃尔薇拉Eduardo Robles Elvira

投票系统公司Agora Voting首席技术官

纪昂·罗德里格斯Keonne Rodriguez

区块链技术公司Blockchain的产品主导人员

马修·罗斯扎克Matthew Roszak

投资机构Tally Capital创始人及首席执行官

科林·鲁尔Colin Rule

电子商务解决方案Modria.com主席及首席执行官

马可·桑托利Marco Santori

美国律师事务所Pillsbury Winthrop Shaw Pittman LLP法律顾问

弗兰克·斯维尔Frank Schuil

瑞典比特币交易平台Safello首席执行官

巴里·西尔伯特Barry Silbert

数字货币集团创始人及首席执行官

托马斯·史帕斯Thomas Spaas

比利时比特币协会主管

巴拉吉·斯里尼瓦桑Balaji Srinivasan

区块链硬件公司21的首席执行官、著名风投机构Andreessen Horowitz合伙人

林恩·圣·阿穆尔Lynn St. Amour

互联网协会（Internet Society）前任主席

布雷特·斯塔普尔Brett Stapper

猎鹰全球资本创始人及首席执行官

伊丽莎白·斯塔克Elizabeth Stark

耶鲁法学院访问学者

尤塔·斯坦纳Jutta Steiner

以太坊/软件公司Provenance

梅拉妮·斯旺Melanie Swan

区块链研究学院创始人

尼克·绍博Nick Szabo

乔治华盛顿大学法学院

阿什莉·泰勒Ashley Taylor

以太坊生态圈区块链公司Conensys Systems

西蒙·泰勒Simon Taylor

巴克莱银行企业合作关系副总裁

戴维·汤姆森David Thomson

艺术家网络Artlery创始人

米歇尔·廷斯利Michelle Tinsley

英特尔公司移动及支付安全部门主管

彼得·托德Peter Todd

比特币公司CoinKite里“专门负责唱反调的人”

贾森·蒂拉Jason Tyra

区块链媒体网站CoinDesk

瓦列里·瓦维洛夫Valery Vavilov

BitFury首席执行官

安·路易斯·韦霍韦茨Ann Louise Vehovec

加拿大皇家银行金融集团战略项目高级副总裁

罗杰·维尔Roger Ver

“比特币先驱”，硬件公司Memorydealers KK创始人

埃克斯利·维尔塔宁Akseli Virtanen

罗滨汉资产管理公司对冲基金经理

埃里克·沃里斯Erik Voorhees

数字货币兑换服务商ShapeShift首席执行官及创始人

乔·温伯格Joe Weinberg支付机构

Paycase联合创始人及首席执行官

德里克·怀特Derek White

巴克莱银行首席设计及数字官

特德·怀特黑德Ted Whitehead

宏利资产管理公司高级常务董事

苏可·威尔科特斯-奥赫恩Zooko Wilcox-O'Hearn

软件公司Least Authority Enterprises首席执行官

卡罗琳·威尔金斯Carolyn Wilkins

加拿大央行高级副总裁

罗伯特·威尔金斯Robert Wilkins

商业工具公司myVBO首席执行官

卡梅伦·文克莱沃斯Cameron Winklevoss

文克莱沃斯资本创始人

泰勒·文克莱沃斯Tyler Winklevoss

文克莱沃斯资本创始人

黄平达Pindar Wong

互联网先锋、安全方案提供商VeriFi主席

加布里埃尔·吴Gabriel Woo

加拿大皇家银行金融集团创新业务副总裁

加文·伍德Gavin Wood

以太坊基金会首席技术官

亚伦·赖特Aaron Wright

美国叶史瓦大学卡多佐法学院教授

乔纳森·齐特林Jonathan Zittrain

美国哈佛大学法学院

同时，要衷心感谢那些投入了精力帮助我们的人。全球解决方案网络项目的安东尼·威廉斯（Anthony Williams）和琼·比格姆（Joan Bigham）与亚历克斯在最初的数字货币治理论文上进行了紧密的合作。前思科高管琼·麦卡拉（Joan McCalla）为物联网及政府和治理这些章节进行了深入的研究。我们也得到了很多来自家庭成员的帮助。IT高管鲍勃·塔普斯科特（Bob Tapscott）花费了很多时间去下载和了解比特币的完整区块链数据，给我们带来了在一些技术问题上的第一手见解。技术企业家比尔·塔普斯科特（Bill Tapscott）提出了基于区块链的个人碳信用额度的革命性构思，而技术高管妮基·塔普斯科特（Niki Tapscott）和她的丈夫、金融分析师詹姆斯·利奥（James Leo）在这个过程中一直都是非常好的参谋角色。塔普斯科特集团的凯瑟琳·麦克莱伦（Katherine MacLellan）处理了一些围绕智能合约的严肃问题（她恰好是一位律师），并管理了采访的过程。菲尔·柯尼耶尔（Phil Courneyeur）每天都在寻找丰富的材料，而戴维·蒂科尔提供了直至目前为止有关数字时代所处的状态的深入见解。演讲者管理机构Leigh Bureau的韦斯·内夫和比

尔·利（Bill Leigh）帮助我们起草了这本书的构思（这已经是第几本书啦，朋友们？）。就如过去的20年间一样，乔迪·史蒂文斯（Jody Stevens）完美无瑕地执行了与整个项目相关的管理工作，这包括处理数据库、财政工作、文档管理、校对及生产过程——这些任务对她而言是一项全职工作。需要注意的是，她在塔普斯科特集团里还有另外的一些全职工作。

特别感谢区块链公司智能钱包公司的首席执行官迪诺·马克·安格里蒂斯、以太坊开发工作室Consensus Systems的首席执行官约瑟夫·卢宾以及正在快速成长中的安全公司WiSeKey的卡洛斯·莫雷拉，他们每一个人都花了不少的时间与我们进行头脑风暴并交换想法。他们都是才华横溢的，也乐意帮助我们。现在我们可以见证他们在这个领域中的事业的成功，这对我们而言是一种享受。另外，我们也非常感谢企鹅兰登书屋的伟大团队，它是由我们的编辑耶西·马士洛（Jesse Maeshiro）带领的，而阿德里安·扎克海姆负责监督工作。

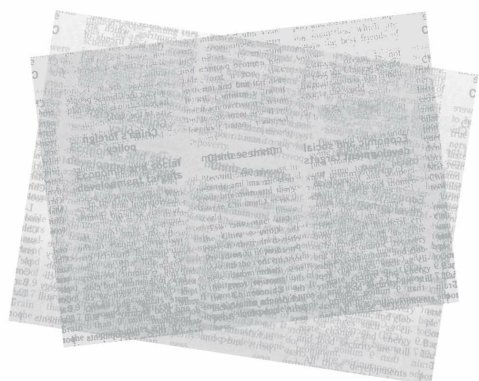
最重要的是，我们衷心地感谢我们的妻子，唐的妻子安娜·洛普斯和亚历克斯的妻子艾米·威斯曼容忍了我们在大半年间对完成这个任务的执着。有这样完美的生活伙伴，我们两人都感到非常幸运。

这本书的写作过程对我们两人来说都是一段充满快乐的经历，可以这么说，我们享受其中的每时每刻。就如某个名人曾经说过的那样，“如果两个人在什么问题上都有着相同的看法，那么其中一个人就没必要存在了”。我们每天都对对方的观点提出挑战，以测试我们的信念和假设，而这本书恰恰是有关这段健康和有活力的协作关系的明证。注意，当两个人共享这么多的DNA（遗传物质脱氧核糖核酸）特征及有着30年共同探索世界的历史，进行协作似乎就是毫不费力的了。我们希望你能意识到这段协作关系所产生的成果的重要性，并能对你有所帮助。

唐塔普斯科特和亚历克斯·塔普斯科特写于2016年1月

第一篇

假如需要变革



第一章

可信的协议

就如历史上反复出现过的场景那样，技术的小精灵似乎又一次从瓶子中被释放出来了。一个（或一群）身份和动机都无人知晓的人，在历史中的一个不确定的时刻里召唤了这只小精灵。现在，如果我们能很好地利用它，这个小精灵或许能为我们所用，带来另一场变革，并有可能革新经济格局和人类社会各种事务的旧秩序。

让我们来解释一下吧。

互联网前40年的发展历史给我们带来了电子邮件、万维网、网络公司、社交媒体、移动网络、大数据、云计算以及物联网的早期生态。它极大地降低了搜索、协作和交换信息的成本。它降低了以下领域的准入门槛：新媒体、娱乐业、新式的零售业、新式的工作组织架构以及前所未有的数字化商业模式。通过传感器技术，互联网将智能整合到我们的钱包、衣物、汽车、建筑、城市甚至是我们的身体上。互联网已经完全渗透了我们所处的环境，在不久的将来，我们就不需要像今天这样“登陆”到互联网上，而是会通过无处不在的（互联网）技术去运营我们的业务及管理我们的生活（持续的在线生活）。

可以这么说，互联网让很多积极的改变成为可能——对那些有着接入互联网条件的人而言更是如此。不过，对商业和经济活动来说，互联网还是存在着很大限制的。《纽约客》在1993年刊登过漫画家彼得·施泰纳的一幅漫画，上面写着“在互联网上，没有人知道你是一条狗”，估计在今天，这句话还是非常贴切的。在互联网上，若没有第三方机构——如银行或政府提供的校验信息，我们依然无法在彼此之间确认对方的身份，也无法在彼此间建立经济往来活动所需的信任关系。问题就出

在这里——这些中间机构恰恰利用了我们中介的需求，为了商业目的和国家安全等理由去收集我们的数据和侵犯我们的隐私。互联网技术改善了信息交换的效率，但即使是这样，这些中间机构所产生的额外成本依然让全球范围内25亿的人群难以负担各种金融服务。互联网曾经给很多人带来了一个期望——建立一个由点对点协议驱动的新世界，但其带来的经济和政治效益已经被证明是不对称的，权力和财富还是流向那些已经有权力和财富的人，即使他们已经没有再积极地努力做出贡献。资本们赚取新财富的速度，比大多数人都快。

相对于技术对隐私所带来的侵害，它所创造的繁荣程度并不能让人感到满意。不过，在这个数字化的时代，无论是好的还是坏的事情，技术已经处于一切事物的中心了。技术让人类更尊重和维护彼此的权利；同样地，技术让人类能够有更多的新方式去侵害彼此的权利。在线通讯以及在线商业的爆发式增长，让黑客们有更多的机会进行网络上的犯罪活动。摩尔定律预测了运算能力每年的翻倍式增长，而这也让诈骗活动和盗窃活动的活跃程度翻倍了，这个现象可用“摩尔的不法之徒定律”¹来描述。至于垃圾信息传播者、身份盗窃者、在网上“钓鱼”的罪犯、间谍、僵尸网络入侵者（被植入恶意软件的机器组成的网络）、黑客、网络恶霸及数据敲诈者（那些用勒索软件去控制他人数据以牟利的人），这些人给互联网带来的影响也非常大。以上提到的仅仅是冰山一角。

寻找可信的协议

早在1981年，一些发明家们就曾经尝试用密码学去解决互联网的隐私性、安全性和包容性的问题。由于第三方机构的存在，无论这些发明家们如何尝试重新设计互联网的基础流程，还是无法完全解决这些问题。在互联网上，用信用卡进行支付是不安全的——这是因为用户需要向第三方透露很多个人数据。另外，对小额支付而言，这个过程也会产

生不菲的手续费。

后来，一个名为戴维·查姆的天才数学家在1993年提出了eCash系统，这是一个数字化支付系统——“在技术上这是一个完美的产品，让在互联网上安全地、匿名地进行支付成为可能.....在互联网上，用它来进行一些价值极低的交易是非常合适的。”²它是如此完美，以至于当时的微软和网景公司甚至有意将其作为一个功能整合到Windows 95和Mosaic浏览器中。³不过，当时的在线购物客们并不关心网络上的隐私和安全问题。戴维·查姆的荷兰公司DigiCash最终在1998年走向破产。

在那段时间里，戴维·查姆的一个同事尼克·绍博写了一篇题为“上帝协议”的简短论文，这题目是模仿诺贝尔奖得主利昂·莱德曼所创的词语“上帝粒子”，象征了希格斯玻色子在现代物理学中的重要性。尼克·绍博在这篇文章中设想了一种无所不能、可以取代所有中间机构的技术协议，即让“上帝”在一切的交易中扮演可信的第三方。其设想如下：“所有的参与方都会将其信息和价值输入到上帝的手中，上帝会可靠地决定执行的结果，并将结果输出到参与方的手中。在这个过程中，一切涉及隐私的信息都归上帝所有，没有参与方能窥视与自己无关的信息。”⁴他的想法是很大胆的——在互联网上开展业务确实是要依靠“信仰的飞跃”。由于现有的互联网基础设施并不能提供必要的安全性，中间人在各种事务中就变得尤为重要了——它就如神一般的存在。

自此，十年过去了。到了2008年，全球金融市场出现了大规模的灾难。凑巧的是，一个（或一群）名为中本聪（Satoshi Nakamoto）的人在这时发布了一种点对点的现金系统及其基础协议，这就是后来被称为“比特币”的加密货币。加密货币（数字货币）与传统的法币有所不同，因为它们不是由国家所创建的，也不是由国家所控制的。这个协议以分布式计算技术为基础设定了一系列的规则——这让在脱离可信第三方中介的情况下，数十亿的设备能够在彼此之间安全地交换信息。这个看似平凡无奇的举动引发了一系列的连锁反应，它使以计算机为核心设

备的世界感到兴奋、害怕，同时，也释放了这个世界的想象空间。它的影响扩展到了全球范围内的商业、政府、隐私保护提倡者、社会发展活动家、媒体理论家和记者等领域和群体——这还仅仅是冰山一角。

“他们的反应是这样的，‘天啊，就是这个了。这就是我们一直在等待的重大突破’”，首个互联网浏览器的创始人、同时也是比特币与区块链相关的风险投资活动的重磅投资者马克·安德森如是说，“‘他把一切的问题都解决了。不管这人是谁，他应该获得诺贝尔奖——他就是个天才’。这就是互联网上一直被需要却又一直没有实现的分布式可信网络。”⁵

今天，世界各地的有识之士正在思考——尝试理解这个仅通过智能代码就能让普通人去架设信任桥梁的协议及其潜在影响。这在以前是从来没有发生过的——在两个或多个参与方之间直接进行可信的交易，而这些交易会通过大规模协作进行校验，并由集体的利己动机驱动，而不是像以前那样由商业化的大公司去驱动。

它或许不是万能的，不过作为一个能让我们进行交易的、可信赖的全球平台，我们并不能低估其影响力。现在，我们将它称为可信的协议。

这个协议是数量正在不断增长的全球分布式账本（被称为区块链）的基础，其中比特币是规模最大的一个。虽然这项技术是很复杂的，而“区块链”这个词也不是广为人知，但其主要的构思是很简单的。区块链让我们可以直接、安全地将钱发送给你，中间无须经过银行、信用卡公司或像贝宝PayPal这样的支付公司。

这已不仅是信息互联网了，这还是价值互联网和货币互联网。它也是让每个人去获取事实真相的平台，至少对它所存储的架构化信息来说是这样的。在底层，它是一个开源代码：任何人可以免费下载、运行和使用它，以开发用于管理在线交易的新工具。因此，它可能释放出无数

的新应用和新潜能。在将来，那些目前还没有实现的潜能将有可能改变一切。

这个世界账本是如何运作的？

大银行和一些政府正在将区块链作为分布式账本实施，以改变信息存储和交易发生的方式。它们的目标是值得称赞的——高速度、低成本、安全性、更少的错误以及移除中心点攻击和故障的可能性。这些模式并不一定内建有助于支付的加密货币。

不过，最重要的、影响力最大的区块链是建立在中本聪的比特币模式之上。下面是它们的工作方式。

比特币或其他加密货币并不是存储在某个地方的文件里的；它以交易的形式存储在一个名为区块链的总账或表格中，这个区块链会利用大范围的点对点网络资源去校验和批准每一笔交易。区块链是分布式的：它运行在由全球志愿者提供的计算机上；黑客们并不能通过入侵某个中心化的数据库去破坏这个系统。区块链是公开的：任何人都能在任何时候查看区块链上的信息，因为它是在网络上存在的，而不是像传统系统那样负责审计、保管记录的中心化机构中。最后，区块链是加密的：它使用了高强度的公钥、私钥加密算法（而不是像保险箱使用的两把钥匙）去维护虚拟世界的安全性。你不需要担心塔吉特百货、家得宝(美国家居连锁店)或美国联邦政府系统里的脆弱的防火墙，也不需要担心摩根士丹利职员可能发生的盗窃行为对系统的影响。

在比特币网络中，每十分钟内，就如网络中的心跳节奏一样，比特币网络在这个周期内发生的交易将会被确认、清算，并存储在一个首尾相连的区块结构上，这样就构成了一个链条。每一个区块都得对此前区块的事实进行确认。这个架构能够为价值交换活动加盖永久性的时间

戳，让任何人都不能篡改这个账本。如果你想盗窃一个比特币，你就必须在众目睽睽之下改写在区块链上的这个比特币的全部历史记录，而这基本上是不可能的。因此，区块链就是一个分布式账本，它代表着一个网络上的共识——每一笔历史交易的来龙去脉都记录得清清楚楚。相对于世界范围的信息互联网来说，区块链就是世界范围的价值账本。它是一个分布式账本，任何人都能下载这个账本，并在自己的电脑上运行。

一些学者认为，复式记账法的发明让资本主义和民族国家得以走向繁华。通过定制相应的程序，这个为经济交易而设的新型数字账本几乎可用于记录一切对人类而言有价值 and 重要的事物：出生证和死亡证、婚姻证书、契约和所有权凭证、教育学位、金融账户、医学流程、保险偿付、投票、食物溯源以及其他能用代码去编写和表达的事物。

这个新型的平台能用于大部分数字记录的实时对账（对事实进行确认）。事实上，在不久的将来，现实世界的数十亿智能设备将能够进行重要信息的感知、响应、通讯和共享工作——从保护我们的环境，到管理我们的健康信息，它们几乎是无所不能的。一个用于连接一切事物的物联网，需要依赖一个能记录一切事物的账本（万物账本）。商业、贸易和经济需要一个数字化清账技术。

所以，为什么你应该关注？我们相信事实能让我们实现自由，分布式的信任则会给各行各业的人们带来深远的影响。作为一个音乐爱好者，或许你想用艺术品作为谋生的手段；作为一个顾客，或许你想知道眼前的汉堡肉来自何方；作为一个移民人士，或许你已经对汇款到家乡所涉及的高昂费用忍无可忍了；作为一个来自沙特阿拉伯的妇女，或许你想买一本时装杂志；作为一名救援人员，或许你需要确定某块土地的主人，这样你才能在地震后帮助他们重建家园；作为一个公民，或许你已经难以忍受意见领袖们缺乏透明度和问责度；作为一名社交媒体的用户，或许你觉得你产生的所有数据对你来说应该是有价值的，而且你的隐私权是不可忽视的。即使是在本书行文之际，创新家们也正为这些方

面的需求创建基于区块链的应用程序。这仅仅是一个开始。

区块链的理性繁荣

毫无疑问地，区块链对每一个机构来说都有着深远的影响，这也是很多聪明的、有影响力的人都对此技术感到兴奋的原因之一。本·罗斯基（Ben Lawsky）还辞去了他在纽约金融服务局的负责人职位，专门创建了一个关于这个领域的顾问公司。他告诉我们：“在五到十年内，金融系统或将面临重大变革，而我想参与到这个改变当中。”⁶布莱思·马斯特斯在她20多岁的时候就成了摩根大通的董事总经理，现在，她也成立了一个专注于区块链技术的初创企业，期望促进产业的转型。《彭博市场》的2015年10月刊将她放在封面并配上“这一切都与区块链有关”的标题。另外，《经济学人》2015年10月刊的封面文章《信任的机器》如是说——“比特币背后的技术有可能改变经济运行的方式”。⁷对《经济学人》来说，区块链技术是“一个如实记录事实的大型链条”。世界各地的银行纷纷组织一流的团队去调查这其中可能存在的机会，这些团队里面还有不少的杰出技术人员。银行家们喜欢安全性、零摩擦及即时交易的概念，但他们中的一些人在开放性、去中心化及新式货币的概念面前退缩了。金融服务产业已经重新打造并私有化了区块链技术，将其称为分布式账本技术，以期将比特币的优点（安全性、速度、成本方面）与一个需要银行或金融机构授权的完全封闭系统结合起来。对它们而言，区块链是一个比它们现有方案更可靠的数据库，区块链是一种让关键利益相关者（买家、卖家、托管人及监管者）保持共享及不可擦除记录的数据库，它能够降低成本、降低结算风险及消除故障中心点。

针对区块链方面初创企业的投资额正在增加，这有点像90年代的互联网公司的投资热潮那样。现在，风投资本展现出来的热情让20世纪90年代的互联网公司投资者也相形见绌。在2014到2015年，就有超过10亿

美元的风投资本涌入到区块链生态系统中，其增长速度差不多每年翻一倍。⁸“我们很有信心，”马克·安德森在《华盛顿邮报》对其进行的一篇采访报道中指出，“在20年后，我们会像讨论今天的互联网那样去讨论区块链技术。”⁹

监管者们对这个领域的关注也很快地提上了他们的议事日程，他们纷纷成立各种专项工作组，以探索这个领域是否有可行的立法方案。俄罗斯政府已经禁止使用比特币了，而阿根廷这样的民主化政府亦是如此（一些人认为，鉴于货币危机在阿根廷频繁发生，该国政府简单地禁止比特币的行为并不明智）。而在西方，一些更为谨慎的政府正投入大量的精力和资源，试图去理解这项技术能如何改变央行的角色和货币的本质，而其对政府的运作以及民主本质的改变亦在考量当中。加拿大央行的副行长卡罗琳·威尔金斯认为各地银行行长们应该考虑将整个国家的货币系统转移到以区块链技术为基础的系统之上。英国央行的首席经济学家安德鲁·霍尔丹编写了一份建立英国的数字货币的提议。¹⁰

这是一个热闹的时期——确切地说，这里面也有不少机会主义者、投机者甚至是罪犯参与进来了。大多数人对数字货币的初始印象是来自于Mt.Gox比特币交易所的破产事件或罗斯·威廉·乌尔布里希的定罪——后者是在线黑市“丝绸之路”网站的创始人，该网站在被美国联邦调查局查封前一直在协助非法药品、儿童色情和武器的交易，其支付系统就是利用了比特币的区块链。比特币的价格一直在剧烈地波动，而比特币的集中程度也是非常高的。一份在2013年进行的调查报告表明过半数的比特币集中在937人手上，不过今天这个数据一直在变化。¹¹

那么，这样一个曾经与色情和庞氏骗局相关联的技术，如何能给各行各业带来有用的东西呢？首先，除非你是一个交易者，否则你要关注的并不应该是比特币这个依然有投机性的资产。这本书介绍的事物是比资产更有意义的，是关于其底层技术平台的用途与潜力。

这并不是说比特币或加密货币是不重要的，虽然有些人正极力将它们的项目与过去的这些涉及丑闻的事情保持距离。这些货币对区块链革命是非常重要的，这在点对点的价值交换（特别是金钱）中处于头等地地位。

在数字化时代达成信任

在商业领域中，信任是对另一方遵循“诚信四原则”去处理事务的期望。这四条原则是：诚实、考虑对方利益、承担责任及透明性。¹²

诚实并不只是一个道德上的问题，现在，它已经是一个经济问题了。若要在雇员、合作伙伴、顾客、股东以及公众之间建立信任关系，组织就必需诚实、准确、完整地将信息与各方交流。组织不应该通过忽略某种事实的方式撒谎，或通过增加事情的复杂程度以达到混淆细节的目的。

在商业领域，**考虑对方利益**通常是指交易方会诚心诚意地进行价值的交换或让渡，而信任关系的建立，需要建立在对各方利益、需求及感受的考虑上，需要在彼此间心存善意。

承担责任意味着对利益相关方做出明确的承诺，并严格恪守该承诺。个人和机构必需展示出他们有信守承诺并承担违约责任的决心，若他们自己能提供相关的证明，或第三方机构的专家能负责对其履约能力进行验证，那就更好了。个人和机构不应该逃避或推卸自身的责任。

透明性意味着以公开透明的方式运作。若外界有“他们在隐藏什么事情”的想法时，这就表明该组织运作的透明度不高，最终可能会失去外界的信任。当然了，各公司的商业秘密和其他专利信息应当受到保护，但当涉及一些与顾客、股东、雇员和其他利益相关方时，还是有必

要建立一个积极的、开放的沟通渠道，才能获取对方的信任。通俗点说，公司应当开诚布公，才能在未来走向成功。

在商界或其他机构中，一场前所未有的信任危机似乎已经出现了。公共关系公司埃德尔曼的《全球信任度》调查指出，在机构（特别是公司）中的信任度已经倒退到2008年经济危机时的低潮。埃德尔曼的调查指出，即使是过去被视为固若金汤的技术性产业（目前还是最受信任的商业领域），在全球的多数国家中也出现了信任程度的倒退，这样的情况以前并没有出现过。在全球范围内，公司高管和政府官员们继续被评为最不值得信任的信息来源，其可信任程度远落后于学者或产业专家们。¹³类似的还有盖洛普民意测试中心在2015年进行的一份调查报告，表明在美国人对机构的信任程度的对比中，商业机构处于15类被调查机构的倒数第2名，仅有不足20%的受访者表明他们对商业机构有相当或足够的信任。在这个排行榜中，美国的国会是最后一名。¹⁴

在区块链出现之前，商业领域的信任关系通常要依赖于正直、诚信的个人、中介机构或其他组织才能建立起来。我们通常对自己的交易对手了解不足，更不用说考察他们是否诚实可靠了。正因为如此，在网上交易中，我们逐渐地对第三方形成了依赖性，让他们负责给陌生人提供担保，并由他们负责维护与网上交易相关的交易记录、执行商业逻辑和交易逻辑。这些强大的中介机构——银行、政府、PayPal、维萨(Visa)、优步(Uber)、苹果、谷歌及其他数字化的巨头占据了其中一大块的价值。

在区块链这个新兴的领域中，信任关系的建立是基于网络甚至是网络上的某些对象。密码学安全公司WiSeKey的卡洛斯·莫雷拉称，新型技术的出现实质上是分配信任的元素，这样的信任甚至能分配给实物。“如果有这样的一个物体，不论它是一个传感器、通讯塔、灯泡还是心脏监测仪，只要它的工作状况不能被信任，或没有付相关的服务费，它发出的请求就会自动被其他物体拒绝。”¹⁵账本自身就是信任关系

的根本依据。[16](#)

需要说明的是，这里的“信任”是与买卖商品和服务、信息的可信性及保护相关的信任，而非在所有商业事务中的信用。不过，在本书中你会读到一个搭载可信信息的全球账本如何能将正直性植入到我们的机构中，并创造一个更安全、更可信的世界。股东和民众将会期望所有上市公司和由纳税人养活的机构至少将它们的金库放到去区块链上运行。这样的话，通过增加了的透明度，投资者们将能看到某个公司的CEO是否应得到巨额的奖金，而选民们将可以看到他们选出来的代表们是否能妥善处理财政款项。由区块链驱动的智能合约将会要求对手方遵守他们的承诺。

互联网的回归

互联网的早期就如年少时的天行者卢克（《星球大战》中的一个角色）一样，人们相信即使是来自艰苦的沙漠星球的儿童都能推翻一个邪恶的帝国，并通过建立一个互联网公司去开创新的文明体系。那显然是很幼稚的，不过很多人（包括一些现在的人）希望互联网展现出像万维网那样的影响，能够逆转某些产业领域的既定格局。在这个格局中，少数人掌握多数的权力，外来的人很难往这个权力架构上攀登，更莫谈推倒它了。与传统的中心化的旧媒体不一样的是，新式媒体是以分布式、中立的形式存在的，每个人都可以成为一个积极的参与者，而不仅仅是被动的接受者。互联网上的低成本、大范围的点对点通信手段能弱化来自阶级的影响，有机会让发展中国家的民众融入全球经济中。在这种模式下，某个人的价值和声誉来源于其做出的贡献，而不是他的身份或社会地位。如果你在印度努力工作，加上你本身是很聪明的话，这些长处都会给你塑造良好的声誉。世界将会变得更扁平化，更符合能者居之的理想，更灵活及更有流动性。更重要的是，技术将能够造福于所有人，

而不只是为了少数人的财富增长服务。

以上提到的这些构想，其中的一部分已经实现了。维基百科、Linux开源操作系统或银河动物园（Galaxy Zoo）天文学星系图像分类项目都是大规模协作的例子。外包行业和联网的商业模式让发展中国家的民众能够更好地参与到全球经济中。今天，20亿的人在进行平等的协作。我们都能享受获取资讯的新方式，这是前所未有的。

不过，帝国们进行了反击，这似乎是一个越来越明显的迹象了。集中在商界和政界的力量根据自己的需要，改写了互联网最初的民主架构的理想。

现在，大型机构已经控制并建立了这种新型的生产和社交工具，这包括其底层基础设施；其巨量的、增长中的数据集；其正日渐用于商业和日常管理的算法；其海量的应用程序（apps）；以及日渐呈现出来的惊人能力，机器学习及自动驾驶汽车等。从美国硅谷到华尔街，到上海，再到韩国首尔，新式的贵族们正利用其既有优势，运用这种前所未有的非凡的技术、其设计目标就是让人们成为高度活跃的经济主体，从而创造出惊人的财富，并巩固其对经济和社会的力量及影响。

早期的数字化先行者们曾警示过将会发生的一些令人担忧的阴暗面，而现状与他们曾经发出的警示已经相差无几了。¹⁷在大多数发达国家里，尽管其国内生产总值有所增长，但就业机会的增长速度一直不如人意。这个世界的财富一直在增长，而社会不公平的程度也随之增加。强大的技术公司已经不再重视过去的那种开放、分布式、平等和带来机会的网络，而是将重心转移到了线上的封闭式系统或专有的、只读的应用程序，这与其他事情一起，就将对话的渠道切断了。企业的力量已经将这些美好的点对点、民主化和开放的技术作为无节制地获取利益的手段。

这样的结果是，经济的力量变得更锐利、更集中及根深蒂固。互联

网原本的构想是将数据更广泛地、更民主地分发出去，但现在大多数的数据已经被少数的实体收集、利用起来，而且这些实体还利用这些数据去控制和积累更多的权力，这对大众来说并不是一件好事。如果你积累了足够的知识及随之而来的权力，你就可以通过产出更多的专有知识去巩固你的地位。无论如何，特权的重要性已经击败了贡献和实效——不管这些特权是怎么来的。

还有，强大的“数字巨无霸”，如亚马逊、苹果和脸书（Facebook），曾几何时它们也是互联网的初创企业，现在正在私有的数据池里收集民众和机构产生的数据，并没有将它共享到网络上。当它们为顾客创造带来很大价值的同时，也使得数据成为一种新型的资产，甚至比以前的资产都更有价值。这种趋势也侵害了我们传统的个人隐私和自主权的价值观。

各国的政府使用互联网去改善运作和服务的效率，不过它们也在部署各种技术去监视甚至是控制民众。在很多民主国家，政府使用信息与通信技术去监视公民、改变公众意见、推动其狭隘利益、破坏权利和自由，最终目的是保留权力。

当然了，实际的情况也不完全符合某些人提出的“万维网已死”的观点。万维网对数字世界的未来是极端重要的，我们所有人应当行动起来捍卫其发展。另一方面，在如万维网联盟这样的机构里，他们的成员也在积极抗争，以让互联网变得更公开、中立及不断进化。

现在，区块链技术提供了一些全新的可能性，甚至有机会改变上述趋势。这个真正的点对点运作的平台，让我们在本书里讨论的很多令人兴奋的事情成为可能。我们可以掌控自己的身份和个人数据。我们可以进行交易，在无须强大的中介机构充当金钱和信息的仲裁者的情况下创造和交换价值。数十亿被排除在经济体系外的人很快有望加入全球经济体系。我们可以保护自己的隐私，并使用自己的信息谋求自身利益。我们可以保证新事物的创造者能够得到来自他们知识产权的补偿。我们或

许不需要通过重新分配财富的方式去解决日益恶化的社会不平等问题，而是通过在一开始就改变财富分配和创造的方式去实现。这样，来自世界各地的人，无论他们是农民还是音乐家，都可以更全面地、更优先地享有他们所创造的财富。这似乎是有无限的想象空间。

若要打个比方的话，比起上帝来说，这更像是《星球大战》里的尤达大师的角色。不过，这个新式的协议，让一个急需可信协作关系的世界看到了曙光，这已经是很了不起的事情了。

你的个人化身及身份的黑盒子

在历史进程中，每一种新式的媒体都让人们跨越了时间、空间甚至是躯体的局限性。这样的能力最终让我们重新审视存在主义者对身份的观点：我们是谁？作为人类，意味着什么？我们如何能对自身进行概念化？就如马歇尔·麦克卢汉观察到的结果那样，媒介最终会逐渐成为信使。人们塑造媒体，并被媒体反过来塑造自身。我们的大脑、机构和社会都在适应这个趋势。

“今天你需要一个授权机构给你提供一个身份认证工具，如银行卡、飞行常客卡或信用卡。” ¹⁸WISeKey的卡洛斯·莫雷拉说。在出生时，你的父母会给你起名字，而在政府注册的产科医生或助产士会给你接生并记录你的脚印、重量和身高，双方对时间、日期和出生地进行确认并在出生证明上签字。现在，他们可以在区块链上登记这个证书，并将其与出生公告和大学基金关联起来。你的朋友和亲戚可以将比特币发送到你的账户上，以资助你的高等教育。这样，你的数据流就开始运行了。

在互联网的早期，汤姆·彼得斯写道，“你就是你自己的项目”。¹⁹他的意思是，工作和职位已经不再是定义我们的唯一要素。现在若要找一

句类似的话，那就是“你就是你自己的数据”。不过这其中的问题正如卡洛斯·莫雷拉说的那样——“现在，身份是你的，但你的身份在世界中的活动所产生的数据却是由他人所掌管的。”²⁰大多数的公司和机构眼中，你就是一堆数据——这些数据来自你在互联网上的活动踪迹。它们收集你的数据并将其变为一个“虚拟的你”，并通过这个虚拟的身份给你提供很多难以想象的便利。²¹不过，这样的便利是要付出代价的，那就是隐私权。我并不赞同那种“隐私权已经没希望了，别执着了”的思想。²²隐私权是自由社会的基石。

“人们将身份看得太简单了”，²³安全专家安德烈亚斯·安东诺普洛斯如是说。我们用“身份”这词去描述自我、这个自我在世界中的映射以及这个自我或其映射所带来的属性。这些信息或许会来源于自然界、国家或私营机构。我们或许会有一个或多个角色，及随之带来的一系列指标。想象一下你的上一份工作——你角色的变换是由于工作需要做出的改变，还是由于你的职位的变化？

想象一下，如果这个“虚拟的你”能真正地被你掌管，那么世界会变成怎么样？这是你的个人化身，它“生活”在你的身份所构成的黑盒子里，你可以从你的数据流中获得经济利益，当有人申请对你的数据进行访问时，你可以决定向对方公开特定的数据。你的驾驶执照为什么要包含除了“你已经通过驾驶考试并且有能力开车”以外的信息呢？想象一下，如果有一个互联网的新时代，你的个人化身能够管理和保护你的黑盒子里面的内容。这个可靠的软件仆人会根据具体的情况向对方公布必需的细节或金额，同时妥善地处理在网络活动中所产生的各种遗留信息，以保护你的隐私权。

这听上去可能像《黑客帝国》或《阿凡达》这类电影里描绘的科幻故事。不过，今天的区块链技术让它有机会成为现实。以太坊生态圈区块链公司共识系统®（Consensus Systems）的首席执行官约瑟夫·卢宾将这个概念称为在区块链上的“永久数字ID和角色”。“在与大学的朋友互

动的过程中，我展示出来的自己与我在芝加哥联邦储备银行演讲时是不一样的”，他说，“在这个在线数字经济里，我会在拥有不同身份的平台展示出我各方面的特质，并与这个世界进行互动。”约瑟夫·卢宾希望拥有一个‘典型的身份’——这个版本的他会缴税、申请贷款及购买保险。“我或许会有一个业务上的身份以及一个家庭里的身份，以与我的‘典型的身份’相关的事务隔绝开来。我或许会有一个游戏玩家的身份，这我是不希望与我的业务身份联系在一起的。我甚至可能会有一个暗网上的身份，永远不会跟其他的身份联系在一起。”²⁴

你的黑盒子可能会包含以下的一些信息：政府颁发的身份ID、社保号码、医疗信息、服务账号、金融账号、文凭、执业证书、出生证明、其他证书以及一些你并不希望公布但想要产生经济价值的个人信息，如性取向或身体状况等，这些都可以用于民意调查或研究性学习。你可以根据特定的目的，在某个特定的时间段将这些数据公布给特定的机构。你可以将你身份属性的一个子集发送给你的眼科医生，以及一个不同的子集发送给你希望进行投资的对冲基金里。你的化身可以替你回答“是与否”的问题，而不需要公布你的实际身份，这些问题可能包括：“你的年龄是21岁还是更21岁以上？你在过去三年内每年收入超过10万美元吗？你的身高重量指数在正常范围内吗？”²⁵

在现实世界中，你的声誉是本地化的，你的本地商店的店主、你的雇主以及在一个宴会上碰到的朋友都对你有特定的看法。在数字经济里，你的化身中不同身份的声誉是“便携”的。这样的便携性将会把世界各地的人们带入数字经济里。在非洲，拥有一个数字钱包和化身的人将可以建立自己的声誉，而这样的声誉往往是在如贷款创业这样的事情上是必需的。“看，这些人都认识我并给我作担保。在财政能力上我是可以被信任的。我是全球数字经济的一个自治的公民。”

身份只是其中的小部分。其他部分是一个身份云，这个身份云是由那些松散或紧密地与你的身份联系起来的信息组成的。如果我们尝试将

这些信息记录到区块链这个不可篡改的账本上，我们就无法理解社交互动的精髓，也会失去“遗忘”这份礼物。人们永远都不应该由自己状态最差的那个时候定义。

走向繁华的目标

这个可信的协议驱动了数十个项目，在这本书中你将会了解到它们的故事。繁荣首先是关于一个人的生存标准。若要实现繁荣，人们必需有手段、工具及机会去创造物质财富及在经济上兴旺发达。不过对我们来说它包括了更多——人的安全性、安全的环境、健康、教育、环境的可持续性、改变和控制自身命运及参与到经济和社会中的机会。为了实现繁荣，一个人至少需要能够接触到一些基本形式的金融服务以存储和创造更多的价值，另外还要有通信及交易工具以接入到全球经济当中，最后是土地所有权及其他合法持有资产的安全性、保护及执行措施。²⁶ 这些以及更多的特性就是区块链所展示出来的潜力。这些故事能让你感受到一种未来——为每一个人带来繁荣，而不只是给富人和强权者带来更多的金钱和权力；你甚至能感受到一个我们能拥有自己的数据并保护隐私权和个人安全的世界；那是一个开放的世界，每一个人都可以为我们的技术基础设施贡献力量，而不是由被围墙包围起来的大公司给我们提供私有的应用程序；那是一个当前的数十亿被排挤在主流经济秩序之外的人群能够参与到全球经济并分享其成果的世界。下面，我们就来给你描绘一下这个世界。

创建一个真正的点对点共享经济

当专家们讨论“共享经济”的例子时，通常会谈到Airbnb(空中食宿)、Uber（优步）、Lyft（打车应用“来福车”）、TaskRabbit（劳务平台“跑腿兔”）以及其他的一些平台。这是一个很好的概念——体系中的

每一个参与者创造并分享价值。不过这些商业模式其实跟“共享”的关系不是太大。事实上，这些商业模式之所以走向成功，恰恰是因为它们并不进行共享——它们是聚合的模式，这是一个聚合经济。Airbnb这个市值250亿美元的硅谷宠儿专门将空闲的房间资源聚合起来。其他的一些业务模式通过它们的中心化、私有的平台将闲置的汽车、设备以及杂务工人聚合起来，并将这些资源转卖出去。在这个过程中，它们为了商业目的进行数据的收集。这些公司在十年前并没有出现的原因是当时并没有技术上的先决条件，如无处不在的智能手机、完整的GPS功能以及复杂的支付系统。现在，通过区块链技术，就有了彻底改造这些产业的技术条件了。今天的曾经的巨型“颠覆者”快要被颠覆了。

想象一下如果不使用中心化的平台，而是用去分布式技术实现的BAirbnb（区块链版本的Airbnb），这样实质上就会是一个由其成员共有的协作组织。当有潜在的租客希望租一个房间时，这个BAirbnb软件就会在区块链上搜索所有的房源，并将符合租客要求的房源过滤后显示出来。由于这个网络会在区块链上存储交易的记录，这样一个好评就会提高房源提供者的声誉度并塑造他们的身份。这样，就不需要由一个中介机构去负责这个事情了。以太坊区块链的创始人维塔利克·布特因称：“大多数技术都是趋向于将自动化的技术应用在边缘的地方去做一些烦琐的任务，而区块链是在中心实现自动化的。区块链不会让出租车司机失业，而是会让Uber失业并让出租车司机直接为顾客服务。”²⁷

以高速、包容的目标重构金融体系

金融服务产业是全球经济发展的动力，但它现在已经存在着不少问题了。其中的一个问题是，这可能是世界上中心化程度最高的一个产业，而且技术变革在其中的进展非常缓慢。由银行等机构组成的旧式金融秩序像一座座城堡一样，不遗余力地维护垄断的体系并给颠覆性的创新设下障碍。这个金融体系同时也是运行在已经过时的技术上，而且是被可以追溯到19世纪的监管规则所治理的。它里面充满了相互矛盾的事

情，发展状态也不平衡，使得其有时运行得很缓慢，经常出现安全性问题，其运作过程对很多利益相关的人来说也非常不透明的。

分布式账本技术可以将很多金融服务从旧式机构的束缚中解脱出来，培育出竞争对手及创新成果，这对终端用户来说是很有好处的。虽然很多人已经能连接上互联网了，但是数十亿人还是被排除在主流的经济体系之外，这其中的原因很简单，金融机构并不将银行业务这样的服务提供给他们，是因为他们对银行来说是一类无法营利及高风险的顾客。通过区块链技术，这些人不仅能被连接起来，更重要的是能被包容到金融活动里面，能够进行购买、借贷及出售等活动，因此也有了一个创造繁华生活的机会。

现有的机构可以将利用区块链技术进行自身的转型——如果它们能找到一个领导者去做的话。这项技术有希望为这个产业带来变革，让其发展得更好——从银行到证券交易所、保险公司到会计事务所、经纪商、小微贷款提供商、信用卡网络、房地产经纪以及金融产业的其他机构。当每一个人都共享同样的分布式账本时，交易结算可以即时完成，而不需要等待几天，每个人都可以看到执行结果。数十亿的人将会受益于这项技术，这样的转型将会解放世界各地的企业家，为他们的事业提供动力。

在全球范围内保护经济权利

财产权与我们的资本主义民主制度有着不可分割的联系——杰弗逊在《独立宣言》的初稿中将生命、自由和对财产权的追求列入了人类不可剥夺的权利中，而不是后续版本中改写成的“对幸福的追求”。²⁸这些有雄心壮志的原则为我们今天在发达世界里享有的现代经济和社会秩序奠定了基础，但直到今天世界上很多人还没法享受到这些权利。这个世界虽然在生命权和自由权的保护问题上有了一些进步，但世界上的大部分财产持有者的房产或土地可能会被腐败的政府官员们肆意地剥夺——

这个过程只需按下中心化的政府产权数据库里的一个软件按钮即可实现。如果没有财产所有权的证明方式，土地所有者不能得到贷款、申请建筑许可证或出售该财产，而且这些财产随时可以被剥夺。这都是通往繁华的障碍。

著名的秘鲁经济学家、自由民主学院主席及世界领先的经济学者赫尔南多·德·索托表示，世界上多达50亿的人口并不能完全地参与到全球化所创造的价值中，因为他们对土地的所有权得不到保证。他认为区块链能够改变这个现状。“区块链的中心思想是商品的所有权可以被交易——不管它们是金融、实体或智力资产。其目标不仅仅是记录这个地块，还记录所涉及的所有权，这样权利的所有人就不能被侵犯了。”²⁹统一的财产权有可能为全球正义、经济增长、繁荣及和平的新议程奠定基础。在这个新的范式里，权利的保护并不是通过枪械来实现的——而是通过技术。“区块链是为一个由现实（而不是虚幻）事物所支配的世界而设的。我认为那是很有意义的。”³⁰赫尔南多·德·索托说道。这是一项去中心化的技术，其中没有中心化的机构去控制它，每一个人都知道其中在发生的事情，它里面的记录会被永久保存起来。

终结汇款的高费用

每一份评估加密货币相关收益的报告、文章或书籍都讨论过在汇款业务上的应用，这是有正当理由的。在进入发展中世界的资金流中，最多的一部分并不是来自外国援助或国外直接投资，而是其身处海外的国民给他们的贫穷国家寄回去的汇款。这个过程需要时间、耐心，有时还需要每星期跑到同样的电汇办事处的勇气（可能坐落在治安不良的地区），每次都要填写同样的文件及支付同样的7%的费用。其实，有更好的途径能够解决这个问题。

去中心化汇兑公司Abra（后文统称“Abra”）和其他的一些公司正在使用区块链来搭建一个支付网络。Abra的目标是让其每个用户都成为一

个出纳员，资金从离开一个国家和到达另一个国家的整个过程只需要几个小时，在以前这是需要一个星期的；在费用方面，这种方案只需要2%而不是以前的7%甚至更高的费用。Abra希望它的支付网络的节点能够超过世界上所有的实体ATM（自动提款机）数量的总和。西联汇款花了150年的时间才在世界范围内达到了50万名代理人，而Abra将会在第一年拥有同样数量的出纳员。

消除对外援助中官僚主义和腐败

区块链能解决外国援助项目上的问题吗？2010年的海地地震是有史以来最致命的自然灾害之一，约有10万~30万的人口遇难。海地政府后来被证明是一个累赘——全球的社区给红十字会捐献了超过5亿美元的资金，而一份事后的调查报告表明，这些资金有不少是被滥用的，一部分甚至直接消失了。

区块链可以在外国援助分发的过程中移除不必要的中间人的角色。其次，区块链作为一个不可篡改的资金流向管理账本，让机构具有更多的可追责性。你可以在智能手机上跟踪你给红十字会捐赠的每一笔钱（从其起点到终端受益的人）；也可以将资金放在托管账号上，在红十字会完成每一个标志性任务后释放相应数额的资金。

让价值的创造者先受益

在第一代的互联网上，很多知识产权的所有人并没有得到适当的补偿。第一个例子是音乐家和作曲家与唱片公司签约了，而这些唱片公司并没有想象到互联网对这个产业带来的冲击。他们并没有拥抱这个数字时代，也没有重新构造其商业模式，逐渐地就将控制权让给了有创新性的在线内容分发商。

我们来看一下主流唱片公司对在1999年创立的点对点音乐文件分享平台Napster的反应。音乐产业里面的在位者们联手起诉这个新企业、其

创始人及其18000位用户，在2001年7月彻底瓦解了这个平台。Napster的一份相关纪录片的导演亚历克斯·温特对《卫报》说，“在大规模的文化转型的事情上，我并不喜欢黑白分明的想法，而在Napster这事上，在‘我可以分享我购买的一切东西’的立场和‘即使你只分享你已经购买的文件，你也是一名罪犯’的观点间之间存在着不少的灰色地带”³¹。

我们同意这个观点。与顾客共同创造价值通常是一个更可持续的商业模式，而不是去起诉他们。这个事件给音乐产业带来了不少的关注，揭露出其过时的营销实践、内容分发的低效率以及被一些人认为是“反音乐家”的政策。

从那时起，情况并没有发生太大的变化，直到现在。我们可以看到英国创作歌手伊摩琴·希普、大提琴家佐伊·基廷及区块链开发者、企业家们在引领实现区块链上的新型音乐生态系统。这项技术有可能颠覆每一个与文化相关的产业，而它所带来的希望是创作者可以根据自己创造的价值得到补偿。

重构作为资本主义引擎的公司架构

为身份、信任、声誉和交易管理而设的全球性的点对点平台的兴起，让我们终于有机会重建公司的深层架构，这个机构会与创新、共享价值的创建甚至是为大多数人享有的繁荣而服务，而不是只为少数的有钱人服务。这并不意味着我们要建造一个收入或影响力较小的小型机构。相反，我们说的是建造21世纪的公司，其中的一些可能是大型的创富创造者，在它们各自的市场都可能会很强大。我们确实认为企业将会更像网络，而不是工业时代的垂直化层级机构。这样的话，就有机会更民主地分发（而不是重新分发）财富。

我们也会带你预览一下智能合约、新型自主经济代理媒介及被称为分布式自主企业的神奇世界，在其中智能化的软件会对很多方面的资源

和权限进行管理和控制，甚至取代公司。智能合约让基于新型商业模式或应用区块链技术改造的现存商业模式基础上的开放式网络化企业成为可能。

让物体活动起来并让它们工作

技术专家和科幻作家们长期期盼着由联网的传感器构成的无缝全球网络可以捕捉世界上的每一场事件、行动和产生的改变。区块链技术可以让事物进行协作，进行能源、事件、金钱这些价值单位的交换，并根据共享的需求和供应信息去重新配置供应链和生产流程。我们可以为智能设备添加元数据，并为它们编程，使得它们能够根据其他物件的元数据进行相互的识别，并根据预先定义好的情况展开行动或做出反应，这个过程无须担心由错误或篡改带来的风险。

随着物理世界的复苏，从在澳大利亚内陆需要电力耕作的小型农民，到世界各地能参与到一个分布式的区块链能源网络的房产所有者，每一个人都有机会走向繁荣。

培育区块链企业家

企业家精神对一个蒸蒸日上的经济体系和一个繁荣的社会是至关重要的。互联网原本应该解放企业家们，为他们提供大公司才有的工具和能力，而无须担心随之而来的陈旧文化、僵化的流程及固定的负担。不过，互联网公司及其创造出来的亿万富翁的耀目成就掩盖了一个令人不安的事实：在过去的三十年间，很多发达经济体中的企业家精神以及新企业的尝试一直在衰退³²。在发展中世界里，互联网并没有为那些受死气沉沉的政府官僚主义影响的准企业家们降低门槛。互联网也没有改变数十亿人无法获取金融服务的现状——而这些服务对创业者来说是必需的。当然了，并不是每一个人都有成为企业家的使命，不过即使是对那些想获取一份体面工资的普通人来说，这些金融服务和工具的缺失及政

府的繁文缛节使得实现这一点也不容易。

这是一个复杂的问题，不过区块链可以在很多重要的方面实现更高的全球繁荣的程度。对那些生活在发展中世界的普通人来说，若他们希望有一个可靠的价值储存方式及与他们所在社区之外的人做生意的话，现在他们只需要有一个联网的设备就可以了。接入到全球经济中，意味着更容易获得新的信用、资金、供应商、合作伙伴和投资机会的来源。哪怕你的才能或资源价值再小，也能通过区块链实现其经济价值。

实现为人民所有并为人民服务的政府

你也要准备好政府及治理领域的大变革。区块链技术已经可能重塑政府运行的方式，并使其变得更高效，成本更低。它也为民主制度自身的改变创造出新的机会——政府如何能够更开放、摆脱说客的控制及以正直的价值观念行事。从投票、获取社会服务、解决社会的一些大难题及让选出来的代表们对其竞选诺言负责等事项，我们可以看一下区块链技术能如何改变作为公民及参与到政治体系中的意义。

新平台的前景与隐患

若这个“裸露”的城市里有600万的人³³，那么这项技术实现其潜力的道路上就有600万个障碍。另外，也有人对此技术持负面态度。一些人称这项技术还没到大规模使用的程度；一些人称这项技术很难使用，而杀手级的应用还在萌芽阶段。其他的一些观点还批评了达成网络共识所需的巨额能耗——当数以千计甚至数以百万计互相连接的区块链每天在处理数十亿的交易时，会是什么情况？到时候网络中会有足够的激励机制让人们参与进来并长期遵守规则吗？他们会不会尝试攫取网络的控制权？区块链技术会导致大量的失业吗？

这些问题应该由领导者和治理者而不是由技术来回答。互联网的第一个纪元得以蓬勃发展，是因为它的核心利益相关方——政府、民间社会组织、开发者和像你我一样的普通人的视野及共同利益。在本书中，我们将会进一步讨论这个新的分布式范式的领导者们将需要如何参与进来，并释放一系列的经济及制度上的创新力量，以确保这项技术能实现其潜力。我们邀请你成为其中的领导者之一。

这本书源自加拿大多伦多大学罗特曼管理学院的一个400万美元的全球解决方案网络（Global Solutions Networks）项目,它的资金主要是由大型的技术公司及洛克菲勒基金会、史考尔基金会、美国国务院及加拿大工业部（一个致力于寻求解决全球问题和治理方案的新机构）提供的。我们都参与到了这个项目当中。唐塔普斯科特创建了这个项目；亚历克斯领导了加密货币方面的项目。在2014年，我们发起了一个研究区块链革命及其对商业和社会影响的一年期项目，并将其成果归纳到这本书中。在这个项目里，我们深入思考了这个新平台能带来的好处及其风险。

如果商业机构、政府和民间团体创新家能够正确实现这项技术，我们就能舍弃一个主要由不断降低的搜索、协调、数据收集和决策制定的成本所驱动的互联网——根本目的是监视、中介互联网上的信息和交易并实现经济利益，升级到一个由不断降低的交易、监管、执行社会和商业协议的成本所驱动的互联网，其根本目的是保护所有交易及价值创造、分发过程的正直性、安全性和隐私性。这是策略上的180度大转弯。这样的结果可以是一个真正具有分布性的、包容性的、授权性的机构所构成的经济体系——最终就是合理的。通过对我们在网络上可以做的事情、如何去做、谁能参与这些问题做出根本性的改变，这个新平台甚至能够移除应对令人烦恼的社会和经济挑战所需的技术性先决条件。

如果我们不能正确地处理这项技术，区块链这个拥有前景的技术将

会受到限制甚至被摧毁。在更差的情况下，它还可能成为强大的机构们用于巩固其财富的工具，或者当这个平台受到黑客攻击时，则可能会成为某种新的监视型社会所用的平台。与此紧密相关关系的技术有分布式软件、密码学、自主运作的代理人甚至是人工智能，这些技术都有可能失去控制并反过来对付人类。

这项技术被延迟、拖延或无法充分利用的可能性是有的。区块链及加密货币，特别是比特币，其影响力已经很大了，但我们并不会预测这项技术到底会不会成功，也不会预测它走向成功需要的时间有多长。³⁴ 预测总是一件有风险的事。就如技术理论家戴维·蒂科尔所说：“我们中的很多人在预测互联网所带来的影响时实在做得很差。ISIS那样类型的不良现象也是被我们忽略的事情之一，而一些极度乐观的预测最后被证明是错误的。”他说，“如果区块链像互联网那样巨型和普遍，我们对其优点和缺点的预测水平可能也会跟当初预测互联网的时候一样差。”³⁵

我们不再预测区块链的未来，而是积极拥抱区块链的未来。我们认为它应该成功，因为它可以帮助我们实现一个繁华的纪元。我们相信经济运行的最佳状态是它为每一个人运行，而这个新的平台是包容的引擎。它极大地降低了像汇款这样的资金传递活动的成本。它极大地降低了拥有一个银行账号、获得信用记录和投资的门槛。而且，它提倡企业家精神及积极参与到全球贸易中。它催生了分布式资本主义而不是一个将资源和资本重新分发的资本主义。

每一个人应该停止与之抗争，并采取正确的步骤参与进来。我们应该利用区块链这项技术为大多数人谋福祉，而不只是为了少数人的眼前利益。

今天，我们都对这个新一代的互联网的潜力感到兴奋无比。我们对正在出现的大量创新成果及其实现繁荣及更美好世界的潜力充满了热情。这本书是我们告诉你该如何对这个下一代的潮流产生兴趣及进行理

解，并采取行动以确保其潜力能实现。

因此，坐下来并继续读下去吧。我们正处于人类历史的关键节点中。

第二章

引导未来：区块链经济七大设计原则

加拿大瑞尔森大学隐私与大数据研究所执行理事安·卡沃基安认为：“自由是建立在隐私之上的。我第一次认识到这一点是在30年前，那时我刚开始参加在德国的各种会议。在隐私及数据保护方面，德国在全世界都处于领先地位，这绝非偶然。德国人民曾饱受希特勒第三帝国摧残，他们曾被彻底剥夺自由，而这一切都是从丧失隐私权开始的。在悲剧结束后，德国人民表示，“决不能再重蹈覆辙”。¹

这么看来，第一代用于保护用户隐私的去中心化点对点计算平台之一Enigma（英格码）的命名就显得颇具讽刺意味了（或非常贴切）。这个名字与“二战”时期德国工程师亚瑟·谢尔比乌斯创建的一种用来转录加密信息的机器的名字是一样的。谢尔比乌斯创建英格码机本来是用于商业用途的：这一设备能够让全球各公司，及时、安全地传递交易机密、股票消息及其他内部信息。在几年内，德国的军队生产出了一个军用版本的英格码机，从而借助无线电将加密信息广播给军队。战时的纳粹党人曾利用英格码来传播战略计划、详细目标信息以及进攻时间。当时的英格码机就是施加痛苦与压迫的工具。

我们当代的英格码则是推动自由与繁荣的工具。全新的英格码由麻省理工学院媒体实验室的盖·斯金德和奥兹·内森创建，它不仅体现了区块链公共账本的优点，即其透明性——它“为诚实行为提供强大的激励机制”，还融入了“同态加密”及“安全多方计算”技术。²简单地说，“英格码会提取你的信息（任何信息），然后打散它们并为其加密，形成零散数据，之后再随机分布到网络节点上。它不在一个地方保存完整数据”，安·卡沃基安表示，“英格码利用区块链技术来嵌入数据，并追踪

所有的数据片段。”³你可以将数据与第三方共享，而第三方在无须解密的情况下也能将这些数据用于计算。⁴如果这个新的英格码网络能够奏效，那么它将改变我们处理网上身份的方法。设想一下现在你自己有一个储存了你个人信息的黑盒子，只有你能控制并访问里面的数据。

不管这听起来有多酷炫，鉴于以下几个原因，我们在前沿的加密技术上还是要步步为营。首先，它需要一个建立一个由参与者组成的大型网络。其次，区块链公司Blockstream的奥斯汀·希尔说过，“密码学是一个你永远不希望使用最新、最先进技术的领域，因为之前每次出现一种大家都觉得安全的新算法，四五年后就会有一些聪明的科学家站出来说这算法有问题，然后整个机制都会被推翻。所以通常情况下，我们会选择保守但已经被确认过的、持久有效的算法。这种东西需要后期很长时间去验证，而比特币的设计就考虑到了这一点”。⁵

尽管如此，这个概念还是值得认真研究的，因为它在隐私、安全及可持续性方面，具有深刻启示。“英格码正在提供它们声称能够确保隐私的技术”，安·卡沃基安说道。“这是一个很大胆的主张，不过这样的东西在这个联网、互联的世界确实有着日渐提升的需求。”⁶

在我们的研究过程中，我们接触到了一些基于区块链的项目，它们的开发者对基本的人类权利的维护有着类似的愿望——不仅是保护隐私和安全的权利，还有财产权、在法律下被视为人的权利以及参与到政府、文化和经济事务中的权利。你可以想象一下，无论我们居住在哪里、出生在哪里，都有一种技术能够保留我们及家庭的选择权、在世界上表达出这种选择的权利以及控制我们自己命运的权利。如果有了这样的技术，我们将可以创造什么样的新型工具、工作机会、新型商业模式和服务？我们应该如何看待这些机会？得益于中本聪的发明，这答案就在我们面前。

七大设计原则

我们相信下一个新纪元将会由中本聪的愿景所启发，围绕一系列的隐含原则所设计，并由那些充满激情而又富有才华的社区领导者实现。

中本聪的伟大构思仅限于货币方面，而不是要创造第二代互联网这样的更高目标。他并没有提到重塑公司、改变我们的机构或者改善文明程度等事宜。不过，中本聪的这一见解，还是体现了其令人惊叹的简易思维、独创能力以及对人类的深刻洞察力。那些读过2008年论文的人，会越来越清楚地意识到，数字经济新时代即将来临。计算与通信技术的融合推动了第一代数字经济的出现，而计算机工程、数学、密码学及行为经济学的结合或许能推动第二代数字经济。

民谣歌手戈登·莱特富特在他的歌中浅唱道：“如果你能读懂我的心，那你一定能读懂我的爱。”自2011年来中本聪就一直处于与外界隔离的状态（尽管这个名字会时不时出现在网络社区讨论板块），不过我们认为，他独创的这套信任协议，为机构及经济的重新组建提供了参考原则。

每个与我们谈论过的人，都迫切地想要分享他们关于区块链技术的见解。我们根据每一场对话、每一份白皮书以及每一个论坛帖子展示出了一系列的主体，而我们将这些主题提炼成设计原则——在区块链上创建软件、服务、商业模式、市场、机构甚至是政府事务方面的原则。虽然中本聪并没有具体提到过这些原则，但它们一直暗含在他发布的技术平台上。我们将其视为塑造数字经济及恢复信任的新纪元所需遵守的原则。

如果你刚刚接触区块链领域，我们希望这些原则有助于你理解区块链革命的基本原理。即使你是一个坚定的比特币区块链的怀疑者，在你以后的企业家、投资者、工程师或艺术家的生涯中，如果你需要与志趣

相同的人进行创意协作；如果你是各种资产的所有者或投资者；如果你是一个希望重新构想你在这个区块链经济的早期所扮演角色的管理者；那么，这些原则对你来说都有一定的参考价值。

网络化诚信

原则：信任源自内在，而非外在。诚信被编码到流程的每一环节中，它是分布式的，而不依赖于任何一个成员。参与者之间能够直接进行价值交换并可以期望另一方以诚信的方式行事。也就是说，诚信价值观——包括言行上的诚实、考虑对方利益、对自己的决定与行为负责及决策与行动的公开透明等——会以编码形式体现在决定权、激励制度以及运作过程中，这样个人或机构就必需以诚信的方式行事，否则就可能耗费更多的时间、金钱、能量和声誉。

有待解决的问题：在互联网上，人们一直无法直接进行金钱交换，这纯粹是因为金钱本质上和其他信息产品或知识产权是不一样的。你可以把同一张自拍照传给所有朋友，但是你付给另一个人的一美元不能再付给你的朋友了。钱必需从你的账户离开并转入你朋友的账户，它不可以同时存在于两个账户中，更不应该在多个账户中了。所以，就有可能出现这种风险，即在两个地方使用了同一个单位的数字货币，并让其中一笔像空头支票那样被退回来。这种就是双重支付的问题。这对那些想重复支付同一笔钱的诈骗分子来说是一件好事。但对那笔无效款项的接受者来说就是一件坏事了，而且还会对你的在线声誉度带来不良影响。在传统情况下，在进行在线支付时，我们会借助第三方中央数据库对每一笔交易进行清算，从而解决双重支付问题，比如通过汇款服务（如西联汇款）、商业银行（如花旗银行）、政府机构（如澳洲联邦银行）、信用卡公司（如Visa），或者在线支付平台（如PayPal）等等。在世界上某些地区，结算可能要花好几天甚至是好几周才能完成。

突破性进展：中本聪利用现有分布式点对点网络及一些聪明的密码学技术创建了一套共识机制，从而以跟可信的第三方相当（或更好）的效果解决多重支付的问题。在比特币区块链上，网络会为所有者花费某个币时涉及的第一个交易盖上时间戳，然后拒绝后来重复花费这个币的交易，这样就消灭了多重签名的问题。网络上运行比特币全节点的参与者叫作矿工，他们负责采集近期交易，以数据块的形式进行结算，并且每十分钟重复执行这一过程。每一个区块必需引用前面一个区块的某些数据才能视为合法。此外，协议还提供了磁盘空间回收渠道，这样所有节点都可以高效地存储完整的区块链了。最后一点，区块链是开放式的，任何人都能见证交易的进行。没有人可以隐藏一个交易，因此追踪比特币比追踪现金还要容易。

中本聪不仅希望去除中央银行的中介角色，也希望去除有关事实记录的含糊及互相冲突的解读方式。让代码来解释一切吧，让网络通过共识算法就所发生的事实达成共识并用密码学在区块链上进行记录。达成共识的机制是至关重要的。以太坊区块链的先驱者维塔利克·布特因在博客中提到：“共识是一个社会过程，即使在缺乏算法帮助的情况下，人类也非常擅长于处理共识问题。”他解释称，如果一个系统的规模超出了人们的计算能力，那么他们就会寻找软件代理人的帮助。在点对点网络中，共识算法分配了对网络状态进行更新的权利，即就所发生的真相进行投票的权利。算法会把这些权利分派给一群构成经济组织的平等对象，这群人在这个体系中有着利益关系。据布特因所言，这个经济组织的一个重要特点是它是以可靠的方式进行分布的：任何个体或联盟都不能控制大部分的权利，即使他们有动机和手段去这么做。⁷

为了达成共识，比特币网络采用了“工作量证明”机制。这听起来有点复杂，但这个想法其实很简单。鉴于我们不能依靠矿工的身份来选择创建下一区块的人，那我们就设置一个非常难（比如它需要耗费大量工作）但是很容易被验证（比如其他所有人都可以快速查阅答案）的谜题。参与者都同意第一个解决问题的人可以创建下一个区块。于是矿工

们必需通过投入资源（如计算机硬件和电力）并找到正确哈希值（有点像一段文字或数据文件的独特指纹）的途径来解决这个难题。他们找到的每一个区块都对应着一定数量的比特币作为奖励。这个谜题是以数学的原理设计的，确保了任何人都没有快速解决的捷径。因此，当网络其他人看到答案时，每个人都会相信这个答案得来不易。此外，根据迪诺·马克·安格里蒂斯所述，这个谜题的过程已经进行到“每秒执行500000亿次哈希运算”的规模。矿工们“都在寻找符合这一要求的哈希值，据统计，这个值每十分钟就会出现一次。这就是个泊松分布过程，有时候只要一分钟，有时候要一小时，不过平均是十分钟一次。”迪诺·马克·安格里蒂斯解释了其运作方式：“矿工把网络中所有待处理交易收集起来，然后通过加密摘要函数来运行数据。这个加密摘要函数又叫安全哈希算法（SHA-256），一般输出32字节的哈希值。如果这个哈希值低于某特定目标（这个目标由网络设定且每隔2016个区块调整一次），那么就说明矿工已经找到了答案，并‘破解’了该区块。但不幸的是，对矿工而言，找到正确的哈希值非常困难。如果哈希值错误，那矿工就得稍微调整输入的数据，然后再次尝试。而每次尝试都会得出一个和之前截然不同的哈希值。他们不得不反复试验，直到找到正确答案为止。截止至2015年11月，哈希值尝试的次数平均达到3.5亿兆次。这个工作量非常大！”⁸

你可能听说过其他共识机制。第一版以太坊区块Frontier也采用了工作量证明算法，不过以太坊1.1版的开发人员想改用“权益证明机制”。权益证明机制要求矿工购入并保留某种形式的价值储存手段（比如点点币、未来币NXT之类的区块链原生代币）。他们不必花费能量去投票。而其他区块链，比如瑞波以及恒星币，它们则要依靠社会网络来实现共识，并且他们会建议新的参与者（比如，新节点）给出一份独一无二的节点列表，这份列表至少包含100个他们所信任的节点，对事务的状态进行投票。这类证明机制会有所偏倚：新来的人需要具备社交治理和声誉才能参与其中。还有一种是“活动证明机制”，它是工作量证明与权益

证明的结合体，在区块被正式承认前，一个随机数量的矿工必需利用加密密钥对一个区块进行签名。⁹而“容量证明机制”就是要求矿工配置超大硬盘空间来进行挖矿。还有一个相似概念，即“存储量证明”，这种机制需要矿工在一个分布式云平台分配并共享磁盘空间。

存储空间是有一定影响的。区块链上的数据和互联网上的数据有很大不同。在互联网中，大部分信息具有延展性并快速流动，而该信息的确切发布日期和时间对过去或将来的信息而言并不重要。而在区块链上，从比特币的产出开始，其在网络中的动向就被盖上戳记。要验证一个比特币，不光要引用其自身的记录，还要参考整个区块链的历史。因此，区块链也必需以完整的方式进行保存。

挖矿过程非常重要，这包括了将交易集合到一个区块里、投入一些资源、解决问题、达成共识及保存完整账本的副本——甚至有人把比特币区块链当成类似互联网那样需要有公众支持的公共设施。安永会计师事务所的保罗·布罗迪认为我们应该把所有电器的处理能力都投入到区块链维护中，他说：“如果你的割草机或洗碗机有一个中央处理器，然后这个中央处理器的处理能力可能是实际所需的一千倍，这样的话为什么不用它来挖矿？这并不是为了赚钱，而是用来维护你在区块链上的权益。”¹⁰除了共识机制，区块链还能通过智能代码来保障诚信，而不是靠人类自己去选择做正确的事。

对区块链经济的影响：我们不用再依靠大公司和机构来验证人们的身份，为他们的声誉进行担保了，取而代之的是我们可以信任网络了。我们有了一个平台，在这个平台中，无论另一方如何运作，都能保证信任，这一点是前所未有的。

对大多数社会、政治以及经济活动来说，其影响是惊人的。信任不仅关乎婚姻嫁娶、投票选举、钱财支付，对那些追求可信记录和交易保障的人来说，它也很重要。比如这个东西的所有权归谁？这是什么东西

的知识产权？谁是从医学院毕业的？耐克、苹果设备还有婴幼儿配方奶粉是谁发明的？这些钻石从哪儿来？信任是数字经济的必要条件，而一个安全可靠的广泛合作平台，或许能够推动新型社会与组织的出现。

分布式发电

原则：系统通过一个点对点网络来分配电力，而不再进行单点控制。任何参与者都无法关闭系统。如果某个体或团体的电源被切断了，系统也还是能够运行。如果有超过一半的网络试图覆盖整个网络，那么每个人都可以看到事情的发生。

有待解决的问题：在第一代互联网中，任何拥有庞大用户基础（可能是员工、市民、消费者或者其他组织）的大型机构，都没怎么考虑过社会契约的问题。中心化的力量一次又一次证明了他们对用户的忽视，他们随意存储并分析用户数据，在用户不知情的情况下把数据提交给相关部门以满足其要求，还未经过用户同意就大范围改变数据。

突破性进展：比特币区块链运作所花费的过高能源成本可能会超出它所带来的财务效益。中本聪采用的工作量证明机制需要用户进行大量运算（这非常耗电）来维护网络运作，从而铸造新币。密码专家亚当·巴克开发了哈西现金（Hash cash）解决方案来减少垃圾邮件以及拒绝服务攻击，而中本聪也从这一解决方案中获得了灵感。亚当·巴克的算法需要发件人发送邮件时提供工作量证明，实际上就给邮件盖上了“特殊递件”的戳记来显示这份信件对发送者重要性——“这份信件非常重要，我花了所有精力来传送给你。”这样一来，发送垃圾邮件、恶意软件以及勒索软件的成本就会增加。

任何人都可以免费下载比特币协议，并且保留一份区块链副本。它利用了一种名为bootstrapping（自展开）的技术，通过一些简单的指令触发程序的其他部分从而把程序上传到志愿者的电脑或移动设备上。它

就如BitTorrent一样是完全分布在一个由志愿者组成的网络上的。它是一个建立在世界范围内成千上万台电脑之上的知识产权的共享数据库。

当然，它确实能使网络免遭干预，不过这一点有利也有弊。在区块链上，再也可能像富兰克林·罗斯福执政时期发布6012号行政命令那样，随意冻结资产。当时的6012号行政命令要求市民要么把所有“金币、金条、黄金凭证”都转交给政府，要么就等着罚款坐牢。¹¹美国乔治梅森大学的乔希·费尔菲尔德直白地说：“以后想对付中间人也沒辦法了”¹²，区块链无处不在，志愿者会保持区块链副本更新，并将多余的计算机处理器的性能用于挖矿，从而实现区块链的维护。区块链中不会有后门交易，每一个交易动作都会在全网广播以供后续校验和验证。整个过程都不会涉及中心化的第三方，也不会在一个中心化服务器中存储任何数据。

中本聪也通过将账本中新区块的创建过程与比特币发行连接起来的方式，将铸币权分发出去，从而将铸币权放到了对等网络中的每一个节点中。无论是哪个矿工，只要是第一个解出难题并提交工作量证明的，就可以收到一些新的比特币作为奖励。这里面没有美联储、中央银行或财政部来控制货币的供给。此外，每个比特币都能直接连接到创世块并追踪到所有后续交易。

这样就不再需要中介机构了。区块链的功能运作是一场完美的大规模协作。你能够控制你的数据、你的财产以及你的参与度。它的分布式计算能力同时让分布式的、集合的人类能力成为可能。

区块链经济所带来的影响：或许这种平台能够为财富创造提供一种新型分布式模式；也或许这类点对点协作能够缓解人类最棘手的社交问题。或许我们应该通过将真正的权力移交给公民的方式解决现在机构中的信任危机甚至是合法性问题，从而为他们带来真正走向繁荣和参与到社会的机会，而不是像现在那样通过公关方面的手段去解决。

把价值作为激励

原则：系统把所有利益相关者的奖励都结合到一起。比特币或者其他有价值代币都是这个系统的一部分，也与声誉度是相关的。中本聪编写了这一软件，用来奖励那些参与其工作的人，而它是属于那些持有并使用其代币的人，这样他们都会认真维护这个软件。这有点像终极版本的电子宠物，区块链就是一个全球分布式的储备金。[13](#)

有待解决的问题：在第一代互联网中，企业权力集中、规模庞大、制度复杂，而且运行不透明，这使得他们从授予其权利的网络中获取了大量不成正比的价值。大型银行对金融系统的利用已经让其几乎到了崩溃的极限，因为“那些为高管和信贷服务人员而设的激励架构必然会鼓励短视及过分忽视风险的行为，”约瑟夫·施蒂格利茨说道。这也包括了“专挑美国最穷的人下手”，他把这个问题总结为：“如果你为人们提供一个不良的奖励机制，那么他们也会做不良的事，而他们是以大家应该预期到的方式行事的。”[14](#)

大型网络公司利用一些零售、搜索或社交媒体方面的免费服务，来换取用户信息。根据安永的调查，近三分之二的调查对象（经理）表示，他们收集消费者信息是用来推动业务发展的，而近80%的经理称，这样的数据挖掘增加了他们收入。但是一旦这些公司遭到黑客攻击，消费者也就跟着遭殃——信用卡和银行账户信息被窃取，他们不得不处理一大堆烂摊子。因此也难怪在同一调查中，近半数消费者表示，在接下来五年他们会逐渐切断这些公司对他们数据的访问渠道，还有超过半数消费者表示，比起前五年，他们现在提供的数据已经越来越少，比如他们删掉了自己在社交媒体上的信息。[15](#)

突破性进展：中本聪希望参与者能够在符合自身利益的原则下行事。他明白博弈论，他知道，没有守护者的网络很容易遭到女巫攻击

（Sybil attacks），这种情况下，节点会伪造出多重身份、稀释权利并且让声誉的价值贬值。¹⁶如果你不知道自己到底是在和三个参与方还是和一个挂着三个身份的参与方进行交易，那么点对点网络的正直性及其节点的声誉就没有很大的价值了。因此，中本聪编写了源代码，这样一来无论人们如何自谋私利，也无论他们的身份是什么，其行为都会给整个系统带去好处，而且反之还能为他们累积声誉度。这一共识机制要求的资源投入及其比特币奖励机制，能够激励参与者做正确的事，让他们变得可靠——因为从某种程度上说，他们的行为是可以预测的。这样女巫攻击在经济上也就不可行了。

中本聪写道：“按照惯例，区块上的第一笔交易是一个特殊交易，它会创建一种由区块创建者所持的新币。这样就为节点支持网络的行为增添了激励机制”¹⁷。比特币是一种鼓励矿工参与到区块创建中并将新区块同前一区块相连的激励机制。那些率先完成区块创建的人能够得到一定数量的比特币。在中本聪的协议中，他用比特币来慷慨地奖励早期采用者：刚开始的四年，矿工成功开采一个区块能收到50个比特币，之后每隔四年，每个区块的奖励就减半到25个，12.5个，以此类推。因为现在他们也持有比特币了，所以他们就有动力去保障平台在长期的成功，购入顶尖装备来挖矿并更高效地花费能量从而维护账本。比特币不仅是对与参与挖矿和交易的一种激励机制，也是对平台所有权的一种体现。分布式用户账户是加密网络基础架构的最基本元素，一个人在持有并使用比特币的同时也在资助区块链的发展。

中本聪选择那些有计算机运算资源的人作为其经济组织。如果矿工想参与奖励系统，就需要投入网络外部的资源——也就是电力。偶尔也会有不同矿工挖到两个容量相当并且同样有效的区块，这样其他矿工就必需选择他们希望在哪个有效区块之上构建新区块。他们一般会选择他们认为赢面较大的区块来构建，而不是在两个区块之上构建，否则他们就得分散运算力去处理几个分叉链条，而这种方法会损失价值。参与者会选最长的链条作为区块链的权威状态，因为区块链越长就代表所投入

的工作量越大。相比之下，以太坊选择“代币持有人”作为经济组织，而瑞波币和恒星币则选择社交网络。

关于这些共识机制的矛盾点是，一个人通过为自身的利益行事，就能为点对点网络提供服务，这反过来会影响个人作为经济组织成员中的声誉。在区块链技术之前，人们很难利用到他们网络声誉的价值。这不仅是因为女巫攻击会让电脑中进驻多个角色。身份具有多面性，它是瞬态的，并且存在微妙差异。很少有人能够看到其所有面，更别说是发现微妙之处和捕捉全过程了。针对不同情况，我们不得不生成文件等相关证明，来证实我们身份的一些细节。“没有证明文件”的人，就不能进入其社交圈寻求合作。在类似Stellar的区块链上，这是个不错的开始，它创建一种永久的数字存在证明并建立其名誉，这种名誉的便携性超出了一个人所在的地理社区。

价值储存方面的另一项突破就是被编码到软件中的货币政策。尼克·绍博写道：“人类至今使用过的所有货币都或多或少的存在安全问题。这种不安全体现在各方面，比如伪造、盗取等，但是最恶劣的，可能就是通货膨胀了。”¹⁸中本聪采取逐步发行2100万比特币来限制供应，从而防止通胀。由于区块中能挖到的比特币每四年就会减半，而且目前的挖矿率是每小时6个区块，所以大概要到2140年这2100万个比特币才会全部投入流通。因此在这个系统中是不会引发恶性通货膨胀或货币贬值这类情况的。

货币不是唯一可以在区块链上交易的资产，“我们才刚开始探讨潜在的领域，”Blockstream的奥斯汀·希尔说，“如果以可以利用网络并向世界展示的应用程序和协议为标准，我们仍处于1994年的时候。‘这是你能做的事情，它们完全是突破性的。’”¹⁹奥斯汀·希尔希望看到不同的金融工具，包括资产证明真伪鉴定到财产证明所有权等等。他还表示，希望比特币运用到Metaverse（一个虚拟世界）中，用比特币换Kongbucks，然后雇佣伊罗·普托塔格尼斯特——小说的主人公，黑客、

武士兼披萨饼快递员——来帮你黑到一些数据。[20](#)或者你可以亲自进入OASIS（一个充斥着各种虚拟乌托邦的世界），在这个世界你真的能找到复活节彩蛋，赢得哈里得的财产，将OASIS的虚拟定位权授权给Google，并且购买一辆无人驾驶车导航到多伦多。[21](#)

当然，还有物联网，通过物联网我们注册设备并为其设置身份（英特尔已经在做这个事情），然后借助比特币而不是各种法定货币来协调支付。奥斯汀·希尔说：“你可以规定所有你想做的新业务，让其在网络中实现相互操作，并且可以使用网络的基础架构，而无须自己建造一个新的区块链。”[22](#)。

和法定货币不同，每个比特币都可分割到八位小数。在一笔交易中，随着时间的推移，用户可以合并、拆分价值，也就是说一个输入项可以在多个时间内，输出多个项，这比执行一系列交易要高效得多。用户可以设置智能合约来计量服务的使用量，并定期进行小额支付。

对区块链经济的影响：第一代互联网错过了这一切。现在的平台中，人们，甚至是物品，都拥有适当的资金奖励，以鼓励大家参与到有效合作中去创造一切。可以设想一下：一个线上讨论小组中的参与者，能够因此有动力去提高他的名誉，其中一部分原因是若有不良行为会让他们付出经济上的代价；太阳能板的点对点网络中，房主能够收到区块链实时补偿，因为他们生产了可持续能源；在开源软件项目中，贡献合格代码的人，开发者社区会为他们提供补偿。这些其实不难实现。[12](#)

安全性

原则：网络中嵌入的安全措施是不会出现单点故障的，它们不光保证机密性，而且保证所有活动的真实性以及不可抵赖性。任何想要参与其中的人都必需使用加密技术（无法选择不使用），如果有人做出鲁

莽的行为，那么其后果也只由当事人本人承担。

有待解决的问题：黑客攻击、身份窃取、诈骗、网络欺凌、网络钓鱼、垃圾邮件、恶意软件以及勒索软件——这些都会破坏社会个体的安全。第一代互联网既没有体现透明性也没有减少违规行为，它并没有加强对个人、机构以及经济活动的安全保护。普通互联网用户一般只能依靠薄弱的密码环节来保护邮件和网上的账户，因为服务提供商或雇主并没有给出更好的保护措施。比如最典型的金融中介机构：他们的特长是金融创新而非研究安全技术。根据身份盗窃资源中心表示，中本聪发布白皮书的那一年，纽约梅隆银行、美国国家金融服务公司

（Countrywide）、通用电气金融等金融企业资料外泄事件中出现的身份盗窃报道，占同年同类报道的50%以上。²⁴截至2014年，在金融领域中这一数据已经减至5.5%，但是在医疗保健领域，资料外泄报道增加到全年总数的42%。美国国际商用机器公司（IBM）总结出了资料外泄的平均代价是380万美元，这意味着过去两年资料外泄带来的总损失至少达到了15亿美元。²⁵每起个人医疗身份诈骗所带来的损失平均接近13500美元，而这类违法事件还在增加。消费者不知道接下来被入侵的会是他们生活中的哪一个方面。²⁶如果接下来数字革命涉及各方之间直接进行金钱交易，那么就必需保证通信不会遭受黑客入侵。

突破性进展：中本聪要求参与方使用公钥基础设施（PKI）来搭建安全平台。公钥基础设施是非对称加密算法的一种高级形式——用户拥有两个功能不同的密钥：一个用来加密，另一个用来解密，因此它们是非对称的。比特币区块链是目前全世界公钥基础设施最大的平民化应用，仅次于美国国防部公共访问系统。²⁷

非对称加密起源于20世纪70年代，²⁸并于20世纪90年因电子邮件免费加密软件获得了关注，例如Pretty Good Privacy（PGP，一款加密软件）。PGP非常安全，但是使用起来也非常麻烦，因为网络中的每个人

都需要使用它，你必须时刻留心自己的两把密钥以及每个人的公钥。它没有重置密码这一功能，如果你忘记了密码，你就得全部重来。根据Virtru公司介绍，“加密邮件的数量正在增加，然而只有50%的邮件是在传输过程中加密，而端对端加密的邮件仍旧很少”。²⁹也有人不采用加密和解密操作，而是采用数字证书（无须加密和解密技术的情况下提供保护信息的代码）去实现这个需求，不过，用户要使用个人证书就必需进行申请（还有付年费），而大多数常见的邮箱服务，比如谷歌、Outlook还有雅虎，它们是不支持这一功能的。

安德烈亚斯·安东诺普洛斯说：“过去的方法都失败了，因为他们缺少奖励机制，而且人们从不把隐私当作维护系统安全的动力。”³⁰比特币区块链几乎解决了所有问题，它为公钥基础设施在所有涉及价值的交易中的广泛采用提供了奖励，这一点不仅反映在比特币的使用上，而且还体现在共享式比特币协议中。我们不需要担心脆弱的防火墙、盗窃的员工或保险金黑客。如果我们都使用比特币，并且我们能够安全地存储并交换比特币，那么同样的，我们也能在区块链中，安全地交换数字资产和高度机密的信息。

这是它的工作方式。数字货币并不是存储在一个文件里的。它是被一个密码学的哈希值所对应的交易而代表的。用户持有可以控制他们自己财产的密码学钥匙，并在相互之间直接交易。这样的安全性也让用户需要确保自己私钥的隐私性。

安全标准是很重要的。比特币区块链在SHA-256上运行，这是一种非常有名的算法，由美国国家标准与技术研究院发布，被认定为美国联邦信息处理标准。为了找到区块的解决方案，需要反复进行这类数学运算——这样计算设备需要消耗大量电力，来解决难题并争取新的比特币。其他算法消耗的能源就相对较少，比如权益证明机制。

本章开头奥斯汀·希尔说过，不要采用最新、最好的算法。奥斯汀·

希尔目前正同Blockstream的密码学专家亚当·巴克共事中，对那些没有采用工作量证明算法的加密货币，奥斯汀·希尔流露出了担忧，他表示：“我不认为权益证明能够奏效。对我而言，那种系统就是让富人更富，而手持代币就能决定共识。工作量证明则是以物理学为基础的系统，我比较喜欢这个算法，因为这个系统和黄金采用了相似的系统。”³¹

最后，最长的链一般也是最安全的链。中本聪区块链的安全主要得益于其相对成熟性以及其建立的字节币用户与矿工基础。入侵这种区块链，需要投入比攻击短链更多的计算力。奥斯汀·希尔说：“不论什么时候，只要有新网络搭建起新的链，那就会有一群人把自己隐藏的计算能力、所有电脑和中央处理器都从比特币挖矿中撤出，目标直指这些新网络，从而操控它们，实质上也就是攻击这些网络。”³²

对区块链经济的影响：在数字时代，技术安全很显然是社会个人安全的前提条件。如今字节可以在我们的防火墙和钱包间传播，而小偷可以从世界另一端盗取我们的钱包，甚至是劫走我们的车。由于我们每个人都越来越依靠数字工具与数字平台，这种威胁也在我们不知情的情况渐渐出现。比特币区块链的设计更加安全，也更透明，我们可以借此来进行价值交易，并保护我们的数据。

隐私

原则：人们应当控制他们自己的数据。他们可以自主决定哪些身份信息、在什么时候、以何种方式、透露多少给其他人。尊重别人的隐私权和与尊重别人的意思是有区别的。这两点我们都需要做到。中本聪去除了人们信任他人的需要，也就去除了沟通交流中对他人真正身份了解的需要。安·卡沃基安说：“我已经和多位工程师还有电脑科学家沟通过了，他们每一个人都告诉我——‘当然了，我们可以把隐私嵌入到数据架构和程序设计中。我们当然可以这样做了。’”³³

有待解决的问题：隐私是人类的基本权利，也是自由社会的根基。在互联网时代过去的25年时间里，公共和私有领域的中央数据库，已经采集到了个人和机构所有种类的机密信息——有些连他们本人都不知道。各地的人都很担心公司会通过数字世界，采集他们的信息来制造我们所说的“网络克隆”。甚至是一些政府也在建设监视国家，比如最近美国国家安全局就通过互联网进行了不正当监视，这是过分使用其监视权的表现。这种行为对隐私构成了两次冒犯，其一是在我们不知情的情况下，或未经我们同意，就擅自收集并使用我们的资料；其二是未能保护好这些具有吸引力的信息不受黑客盗取。“这不是零和博弈，不是非此即彼的选择，也无关输赢，你可以对一样东西感兴趣，也可以对另一样东西感兴趣。但是这对我来说已经过时了，而且根本达不到预期目标，”安·卡沃基安说，“我们用一种正和模式取代了它，从本质上说，这种模式能够让你拥有隐私，并且填补空白信息。”³⁴

突破性进展：中本聪没有为网络层设置身份认证要求，这意味着在下载并使用区块链软件的时候，所有人都不需要提供姓名、电子邮箱地址或其他个人数据。区块链无须了解每个人的身份。（而且中本聪也不需要获取他们的信息来出售其他产品，他的开源软件将意见领导营销的手段发挥到了极致。）全球银行间金融电讯协会（SWIFT）的运行模式是——如果你用现金付款，SWIFT一般不会要求身份验证——但是我们认为许多SWIFT办公室还是有监视的渠道，而且金融机构要加入并使用SWIFT的话，就必需符合反洗钱以及客户识别规定的要求。

此外，身份识别及验证层同交易层是分离的，也就是说，对于比特币从甲方地址转移到乙方地址这个过程，甲方会进行广播，而交易过程中不会提及任何人的身份。之后网络会证实甲方的确控制这一批比特币，而且甲方已经批准这笔交易，之后再把甲方的信息标为“未使用交易输出项”，并与乙方地址关联起来。只有在乙方要使用这一笔比特币时，网络才会确认现在这些比特币由乙方控制。

我们可以将其和信用卡使用做个比较，信用卡的模式是以身份为绝对中心，所以每次数据库资料外泄，就有几百万人的地址和手机号被盗。最近一些数据外泄事件中涉及的记录数目如下：T-Mobile，1500万条记录；摩根大通，7600万；蓝十字与蓝盾协会，8000万；易趣，1.45亿；联邦人事管理局，3700万；家得宝（美国家居连锁店），5600万；塔吉特公司，7000万；索尼，7700万；还有一些小型资料泄露事件，包括航空公司、大学、天然气和电力公司，还有医院设施公司，这些都是我们最宝贵的基础设施资产。³⁵

而在区块链上，参与者可以选择保持一定程度的匿名性，这样他们就不需要附加其他与身份相关的具体信息，或在中央数据库中录入这些细节。这一点有多重要，我们就不再强调了。区块链上不会放置对别人有吸引力的大量个人数据。通过区块链协议，我们可以选择某项交易或某个环境中，我们能接受的隐私级别。这能帮助我们更好地管理身份信息，并维护我们同世界的交流。

身份识别初创公司“个人黑盒子”（Personal Blackbox）的目标就是帮助大型企业转变其消费者数据关系。个人黑盒子首席市场官哈洛克·库林告诉我们：“像联合利华或保诚集团这样的公司正在联系我们，希望采用我们的平台。他们对建立更好的数据关系很感兴趣，并且非常想减轻现在担负的数据责任。显然他们已经意识到了，数据逐渐成为公司内部的有毒资产。”³⁶这个平台可以让客户访问匿名数据——就像临床试验中，药剂师只知道与患者健康相关的信息一样——而不用承担任何数据安全风险。一些消费者可能用比特币或公司提供的其他好处而将自己的信息让别人观看。在后台，个人黑盒子平台采用的是公钥基础设施，因此只有消费者能够通过私钥访问到他们的数据。甚至连个人黑盒子自己都无法访问到客户数据。

区块链的平台可以提供相对灵活的选择和匿名证明的形式。奥斯汀·希尔把它比作互联网，他说：“一个TCP/IP（传输控制/网络通信协定）

地址并不能视为一个公共ID（身份）。网路层本身并不了解。任何人都能加入互联网，获得IP地址，并且自由地在全世界范围内收发数据包。在社会中，我们已经发现了这样层次的匿名性质所带来的巨大好处.....比特币的运行方式就和这个差不多。网络本身不会强制要求身份认证。这对社会和正确的网络设计来说都是好事。”³⁷

因此虽然区块链是公共的——任何人在任何时候都可以进行浏览，因为它就存在于网络上，而无须由中心机构进行交易审计、数据记录——但是用户身份是匿名的。这也就意味着，如果你想知道特定的公钥持有者是谁，你就不得不对数据进行大量三角定位。发送人可以只提供收件人需要了解的元数据。而且，任何人都可以拥有多个公钥/密钥集，就像他们可以拥有多个设备和网络接入点以及各种不同化名的电子邮箱地址一样。

也就是说，类似时代华纳这种负责分配IP地址的互联网服务提供商，确实会保留身份与账户的关联记录。同样的，如果你从比特币交易所Coinbase这类授权在线交易所中获得比特币钱包，那么这个交易所就必需按照客户识别和反洗钱要求进行严格评估。举个例子，这是Coinbase的隐私政策：“我们会收集你们电脑、手机或其他设备传来的信息。这些信息必需包括你的IP地址、设备信息（包含但不限于标识符）、设备名称及型号、操作系统、位置、移动网络信息以及标准网络日志信息（比如浏览器种类、进出我们站点的渠道和访问我们网站的页面）。”³⁸所以，政府能够传讯互联网服务提供商，并交换这类用户信息，但是他们无法对区块链进行传讯。

还有一点很重要——只要所有利益相关者同意，我们就可以让任意交易、应用程序或者业务模式做到更加透明。我们会在各种情况中，见识到完全透明化后所展现出新性能。公司对消费者、投资者，或者生意伙伴说真话，其实就是在建立信任。³⁹而这就是个人隐私的体现，是组织、机构和公职官员工作透明的体现。

对区块链经济的影响：当然，区块链阻止了“监控社会”的蜂拥出现。现在，我们来思考一下每个人所面临的企业大数据问题。如果企业拥有你全部信息将意味着什么？我们进入全球互联网时代已经20多年了，现在企业能够了解到我们个人生活最隐秘的细节——而这还只是刚刚开始，很快我们的个人健康和健身数据、日常来往、家居生活等所有你想得到的事，都将被人窥探到。很多人还没有意识到自己每天在网上签订“浮士德契约”。消费者通过简单地使用网页，就授权了这些网页的所有者将数字的零散信息汇聚成详细的路线图，从而让它们可以用于商业用途。

除非我们转变到新的范式，否则这不是科幻小说，我们无法预见未来是否会有数亿个体的数亿个替身在数据中心谈笑风生。通过区块链技术，你可以拥有你的个人身份，就像你在《第二人生》虚拟世界里一样。那个虚拟的你会保护你的个人信息，只有在社会或经济交往中得到你同意的前提下才会透露部分所需信息，并确保只要你的数据给别人带去了价值就能收到一定的补偿。这是从大数据到私人数据的转变。可以将这称为“小数据”。

权利保护

原则：所有权公开透明且可执行。个人自由是可以被承认和尊重的。我们坚持这一不证自明的真理——所有人具有与生俱来不可剥夺的权利，这些权利应该也能够受到保护。

有待解决的问题：第一代数字经济主要致力于寻找方法来更有效地行使这些权利。互联网成了新形式的艺术、新闻和娱乐的媒介，供人们进行诗歌、歌曲、故事、照片、音频、视频等版权的创造。我们也能够把现实领域所采用的统一商法典应用到网络上，让其执行在现实世界已经有的功能，目标是消除针对某一物品的交涉及合约创建步骤，不管这个物品价格有多低（比如一支牙膏）。可是即便如此，我们也不得

不依靠一个中介来管理交易，而这些中介有权否认交易，推迟交易，并且把这笔钱存在自己账户上（银行人员把这笔款项叫作“浮款”），或先执行交易但一段时间后就回撤交易。他们预料到了作弊者所占的比例，并接受了一定数量的作弊者的存在确实是无法避免的现状。

效率确实大幅提升了，可合法权益却遭到了侵害，这不仅包括隐私权和安全权，还包括名誉权以及平等参与权。人们可以匿名地对我们进行审查、污蔑与妨碍，而他们自己却只要承担很小一部分风险与损失。电影制作者主要依靠企业联合赞助、视频平台点播、后期DVD销售以及有线电视播放权等来赚取收入。但是他们发现，几十年前发行的影片收入变得越来越少。因为粉丝把电影的电子档都上传到了网上，这样大家就能免费下载。

突破性进展：铸币所需的工作量证明还要求交易附上时间戳，这样一来，就只有第一个使用代币的人能够进行清算与结算。这意味着区块链——同公钥基础设施相结合——不仅仅能防止二次使用，还能够证实流通中每一货币的所有权，而且每一笔交易都不可改变、不可撤回。换言之，在区块链中，我们不能用不是我们的东西进行交易，无论是不动产、知识产权、还是人格权利。此外，如果未经授权，我们也不能以机构代理角色，代表他人进行交易，包括律师或公司经理等。

“个人黑盒子”公司的哈洛克·库林说：“人类社会交流几千年来，每次我们剥夺人们的参与权，他们都能回来并破坏这个系统。我们认为，即使是在数字世界，盗窃他们的自主同意权也是不可持续的。”⁴⁰区块链作为涵盖一切的账本，通过存在证明这样的工具能够充当一个公共登记中心，这就是一个站点，用来在区块链创造并注册契约、产权、收据、许可等对象的加密摘要。“存在证明”不会保存任何源文件副本，文件的哈希值是在用户机器上进行运算，而不是在“存在证明”站点内，因此确保了内容的机密性。即使一个中心化的权力机构关闭了“存在证明”，这些证明还在区块链上。⁴¹这样，区块链提供了证明所有权及在无须审查

的情况下保留记录的方法。

在互联网上，我们不能真的执行合约权利或者对其实施进行监督。所以，针对涉及多项权利并有多方参与的复杂交易，就由智能合约——即包含特殊目的的一组代码——来执行区块链上复杂的指令。“软件与法律描述的十字路口是基础，而智能合约就是踏上这条道路的第一步，”自我感知系统（Self-Aware Systems）的智囊团主席史蒂夫·奥莫亨德罗说，“当如何将法律代码数字化的原则变得更容易理解后，那么我认为各个国家都将开始这一工作.....每个辖区都能明确地实现法律代码化、数字化，而且法律间会有翻译程序.....去除所有法律摩擦问题将会是一个巨大的经济效益。”⁴²

智能合约会通过某种途径为另一方提供使用权，就像作曲家把完成了的音乐作品发给唱片公司一样。合约代码会包含期限、版税以及终止合约的相关条款。发行公司要在规定期限内将版税转到作曲家的比特币账户中。例如，如果作曲家的账户连续30天收到的款项都小于四分之一一个比特币，那么所有权利就会自动转移回到作曲人手里，发行方则无法再获得作曲家登记在区块链上的作品。这一智能合约的执行，需要作曲家和发行方（以及或许是发行公司的财务和法律团队代表）用它们手中的私钥进行签署。

此外，智能合约还能为资产所有者提供一个渠道，从而在区块链上集合资源、成立公司，其间公司条款都会被编为合约代码，清楚地记录并执行所有者的权利。相关机构的聘用合约会规定管理人的决定权，即通过编码来规定在没有所有权许可的前提下，他们能利用公司资源做什么以及不能做什么。

对于保障合约合规性这一点来说（包括社会契约），智能合约提供了一种史无前例的方法。“如果你能通过一种特殊的控制结构来进行一场大型交易，那么你在任何时期都可以预测出其结果，”安德烈亚斯·安

东诺普洛斯说，“如果我有一笔交易完全通过了验证，并且这笔交易的多方签名账户中涵盖了多个签名，那么我就可以预测这笔交易是否能通过网络验证。如果通过了，那么这一交易的金额就可以被领取且不可回撤。所有中心化权力机构或第三方都不可以撤销这一交易，也没有人能绕过网络共识。这在法律和金融领域都是一个新概念。比特币系统为一个合约的执行结果提供了很高程度的确定性。”⁴³

这个合约无法被扣押、中止或者重新转到不同的比特币地址。无论发送地址是哪里，无论采用何种媒介，你只需要把签署过的交易传输到任何比特币网络节点中就可以了。安德烈亚斯·安东诺普洛斯说：“就算人们关掉互联网，我仍旧可以通过短波无线电以摩斯代码的形式传输交易。政府机关可能会审查我的通信记录，但我可以在Skype上用一系列表情符号传输交易。只要另一端的人能够解码交易，并记录到区块链上，那我就能让‘智能合约’生效。也就是说，我们把一些法律意义上很难担保的东西，转变成了可以进行验证并且具有数学确定性的东西。”⁴⁴

在考虑实物产权以及知识产权时，BitPay执行总裁斯蒂芬·佩尔表示：“所有权只是政府或某一机构颁发的一种认证，即承认你确实拥有某物，而且他们会捍卫你的所有权。它就是由任意权威机构签署的一纸合约，用来保障你的权利的。机构会根据你的身份进行签署，而你拿到合约后，所有权就被记录在册，之后你有权将其转交给其他人了。这个过程简单明了。”⁴⁵根据诺贝尔经济学奖得主埃莉诺·奥斯特罗姆的金字塔形权利关系（按强弱顺序排列）来看，共享资源社区也可以考虑采用这种权利分布。在最底层，是授权用户，他们可能只能访问并提取资源；然后是申请人，他们也有这些权利，但他们还能排除他人访问这些权利；经营者除了上述两个权利，还具有管理权；而所有者享有的权利则更多，能够访问、使用、排除他人、管理和出售这些资源（如转让权）。⁴⁶

下面再来考虑隐私权和宣传权，“个人黑盒子”公司的哈洛克·库林

说：“我们的模型就是针对市场权利的。”他们公司采用区块链技术来代表并执行个人权利，从而再从他们个人数据中提取价值。“区块链给我们带来了一大群人，他们因任务和技术聚集到一起，创造各种途径，让企业利用到这些独特的数据库，而不是保护它们的数据孤岛。”⁴⁷简单地说，人们自己创造的数据，比那些公司追踪到的数据还要好，而且在感情色彩上，比起公司，消费者更容易与品牌站一起并影响他们身边的人。

对区块链经济的影响：作为一种经济设计原则，权利的执行始于对这一权利的阐明。在经营管理学领域，全体共治是一个非常有趣（也具有争议性）的行动方案——组织成员会先规定需要完成的工作，再分配权利及职责，然后分头行动，各司其职。⁴⁸那么公司里谁来决定并安排这一系列活动呢？这个问题的答案会编写到智能合约中，然后存放在区块链上，这样整个目标决定、执行过程、奖励机制就能够在达成共识的同时，实现完全透明化。

当然，这不仅仅是技术问题。它远远超出实体资产、知识产权或“个人黑盒子”公司为卡戴珊家族将形象权的模块添加到其隐私保护工具的范畴。我们需要增强对权利的了解，需要形成对权利管理系统的最新认识。一些初创公司正在努力开发一套权利仪表板（一览表），从而反映人们的公民参与度，其中一个度量指标是投票，而其他的指标还有投入技能、声誉、时间以及比特币，或者提供实体产权、知识产权的免费访问权等。让我们拭目以待吧。

包容性

原则：经济发展的最佳状态就是它能兼顾到所有人。也就是说，要降低对参与者设定的门槛，要为资本主义分布式发展创建平台，而不仅仅是重新分配式的资本主义。

有待解决的问题：第一代互联网为人类创造了诸多奇迹。但正如我们发现的，其实世界绝大多数人仍无法使用一些技术，也无法访问金融系统及享受到经济机会。还有，那种声称要让这一新型通信媒介惠及所有人的承诺也只是空头支票。没错，它确实为发达国家公司的新兴经济体带去了数百万个就业岗位，也确实为企业家创业降低了门槛，而且还为弱势群体提供了机遇与基本信息。

但这些还远远不够。如今还有20亿人⁴⁹没有开设银行账户，在发达国家，由于社会不平等现象持续出现，繁荣程度也在下降。在发展中国家，手机常常是人们唯一买得起的通信工具。大多数金融机构都有移动支付程序，这种程序将摄像头和二维码结合在一起。但是，支撑这些中介所涉及的费用使小额付款变得不切实际。最低账户余额、最低支付金额或者使用这一系统的交易手续费等，对处于金字塔底端的消费者来说依旧负担不起。其基础设施成本使得小额付款以及小额账户的设想就此幻灭。

突破性进展：中本聪设计的系统在互联网堆栈顶层运行，但是如果有需要的话，它也可以脱离互联网运行。中本聪设想的是，某个人会通过他所谓的“简化的支付验证”（SPV）模式同区块链进行交互——在手机上也能运行该模式来调动区块链。现在任何人拿着翻盖手机，就可以以生产者或消费者的身份参与到经济或市场中。区块链技术的使用不需要提供银行账户、公民证明、出生证、家庭住址、稳定的当地货币之类的信息。区块链技术将大幅降低汇款等资金传输的成本，并降低银行开户、信用获取以及投资的门槛。而且，区块链还会支持人们创业并参与到全球贸易中。

这是中本聪的部分设想。他知道发展中国家人民的状况还要糟糕。某些出现问题的国家，需要资金来维系运作，于是就简单地印刷更多货币，然后从生产成本和货币面值中赚取差价——也就是硬币铸造税。货币供应量增加其价值就降低。如果当地经济真的崩溃了——就像阿根廷

和乌拉圭，以及最近的塞浦路斯还有希腊——这些机构可能就会冻结那些无法提供“贿赂”的人的银行资产。考虑到这种可能性，有钱人会把资产存放到更值得信任的地区，或换成更加稳定的货币。

而穷人就没法这样，他们拥有的任何资产都会变得毫无价值。官员可以大肆从外国援助中攫取利益，将用繁文缛节封锁本国边界，阻止任何希望帮助它们的人民的尝试。这些人民中，有需要食物和药品的妇女儿童，有饱受战争摧残的难民，也有忍受常年干旱或其他自然灾害的灾民。

澳大利亚小额支付服务商mHITs（Mobile Handset Initiated Transactions的简称，即移动终端发起的交易）发行了一项新服务BitMoby——它可以让100多个国家的消费者，通过短信给mHITs发送一定量的比特币，从而完成手机充值。⁵⁰比特币核心开发者加文·安德烈森说：“你不会看到每一笔交易，你只会看到你所关心的交易。你也不用花钱去相信别人，你只要相信他们会通过网络传递给你想要的信息就可以了。”⁵¹

奥斯汀·希尔认为：“在新兴世界，财产记录是与贫困相关的一个大问题，挖掘区块链在财产记录方面的潜能非常重要。现在没有一个可靠的实体来管理土地所有权。如果能让人们由衷地说出他们拥有哪片土地，并让他们用这片地做抵押，从而改善全家的生活状况，这将会是一个非常棒的用例。”⁵²

从技术层面考虑，加文·安德烈森参考了互联网带宽的尼尔森定律，即高端用户带宽每年会增加50%，而普通群众带宽则会滞后两到三年。带宽落后于电脑处理能力，后者每年能增加60%左右（根据摩尔定律）。因此根据尼尔森所言，带宽是主要控制因素。⁵³大多数设计——包括界面、网站、数字产品、服务、组织等等——都需要适应大众所需的技术，从而发挥网络效应。因此，包容性就意味着要技术覆盖要全

面，不仅仅要惠及处于科学前沿的高端用户，还要惠及世界边远地区穷困人民，考虑到他们科技发展较慢及偶尔还会出现断电等情况。

对区块链经济的影响：在本书后半部分，我们会回答与繁荣相悖的问题——第一代互联网为西方国家带去了繁荣，但是大多数人的生活却并没有提高，这说明互联网还存在很多问题。繁荣的基础是包容，而区块链能够帮助其实现。我们需要明白，包容包含了方方面面。它意味着社会霸权、经济霸权、种族霸权的终结，也意味着健康歧视、性别歧视、性别鉴定的终结。一个人居住的地方、他是否在监狱中过了一晚及一个人如何投票，这些事情都可能给一个人带来访问某些资源的障碍，它也意味着要消除这些障碍，并移除那些无形的障碍及无数的变量。

设计未来

和安·卡沃基安的对话激励了我们，我们要继续完成德国“绝不重蹈覆辙”的抱负。还记得德国联邦总统约阿希姆·高克在希特勒政权的受难者纪念日当天的发言，他说：“我们的道德义务不能单单靠纪念来完成。我们要永远记住纪念日给我们下达的任务。这个任务要求我们保护人类，维护人权。”⁵⁴他的话是在暗指德国人民在宣誓“绝不重蹈覆辙”后，叙利亚、伊朗、达尔富尔、斯雷布雷尼察、卢旺达和柬埔寨地区发生的种族屠杀？

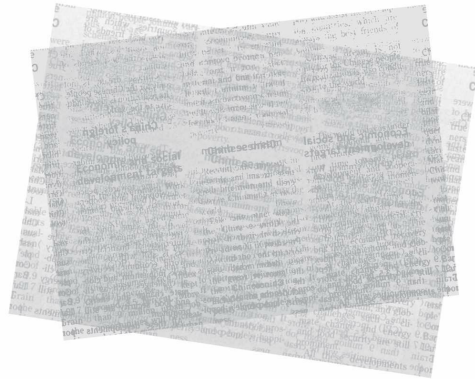
我们相信区块链技术是保护人类，维护每一个人的权利的重要手段，也是沟通真理、传播繁荣的重要手段。它也是拒绝社会中那些可能会以无法想象的方式生长的阴暗面的手段（就像这个网络拒绝虚假的交易一样）。

这的确是非常大胆的言辞，不过至于是非对错，还得读者自行审

视。

从更狭隘且更实际的角度来看，这七大原则能够成为设计下一代的高效能及有创新精神的公司、组织及机构的指南。如果我们的设计能够融入诚信、力量、价值、隐私、安全、权利保护以及包容性等元素，那么我们的经济和社会机构就能重建信任。下面，我们就来看看这些问题该如何深入，对你而言又该做些什么。

第二篇 转型



第三章

重塑金融服务形象：从赚钱机器变成致富平台

全球金融系统每天要转移数万亿美元，为数百万人服务，并为总值超过100万亿美元的全球经济提供支持。¹这是全球最具影响力的行业，是全球资本主义的根基，其领导者被称为“宇宙的主宰者”。然而，在近距离了解这一行业后，你就会发现它是一个由不平衡的发展及匪夷所思的矛盾所构成的复杂机器。首先，这个巨型的机器已经很久没有进行过更新了，新出现的技术一直被匆匆忙忙地添加到日渐老化的基础设施中。你可以想象一下这样的场景，就是银行一边提供网上银行服务，一边继续提供纸质支票，然后还运行着20世纪70年代发明的大型计算机。如果有消费者要刷信用卡购买星巴克大杯拿铁咖啡，那么这笔钱至少要经过5家不同的中介才能最终汇到星巴克的银行账户。交易清算只要几秒时间，但是之后的结算要好几天才能完成。

像苹果和通用电气这样的大型跨国公司，就不得不在世界各地维护所在地的本地货币银行账户，从而推动业务运营。²这些公司需要在其位于不同国家的分支机构间转移资金时，一家分支机构的经理会从该公司的银行账户电汇到另一家分支机构的账户。这些转账过程过于复杂，而且要花很多天甚至是几周来结算。在结算期间，两家子公司都无法动用这笔钱来维持运营或进行投资，而中介机构则可从这笔流动资金中赚取利息。花旗银行前首席执行官维克拉姆·潘迪特说：“技术的出现实质上是将纸面的运作过程转换成半自动化的、半电子化的过程，但是整个逻辑还是以纸质文件为基础的。”³

其他怪异的矛盾点无处不在：交易者在世界各证券交易所进行证券买卖只需几纳秒时间，他们的交易清算能够立即完成，但是结算却需要

整整三天时间。政府发行市政债券的时候至少要使用十类不同代理——包括顾问、律师、保险公司、银行家还有其他相关人员。⁴洛杉矶的一个临时工在某货币市场花5%的费用换到了现金工资，之后攥着这些钱走到便利店，并将钱电汇给远在危地马拉的家人，而这个过程又要涉及固定的费用、汇率及其他隐藏的成本。而家庭成员分完这些钱后会发现，每人分到手的钱根本不够资格在银行开户或办信用卡。他们就是那些每天生活费不到两美元的22亿人口之一。⁵他们要支付的金额太小，对如借记卡和信用卡这样的传统支付手段来说也是非常小的，而这些支付系统中涉及的最低费用也使得所谓的微支付不可能完成。根据近期哈佛商学院一项研究显示，银行根本不把为这类人提供服务看成是一个有利可图的事情。⁶所以，无论是从规模和覆盖范围来看，这个金钱的机器并不是实现真正的全球化。

由于许多大型财政机构的不透明以及监管责任的划分，使货币政策制定者和金融市场监管者缺乏对所有实情的了解。2008年全球金融危机就是一个例子。过度杠杆政策、缺乏透明性，还有扭曲的奖励机制所带来的自我满足感蒙蔽了众人的双眼，而当他们意识到问题的时候，一切都晚了。赫尔南多·德·索托沉思道：“如果你没有相关的数字和地点，你如何能让从警察体系到货币系统在内的任何事情良好地运行？”⁷而监管部门还在使用为工业时代而设的规章制度来管理这台机器。在纽约州，其货币转移相关法律可以追溯到美国内战时期，当时的钱财主要通过马匹和马车来运输。

这是一种“转基因”金融，它充满了荒谬的矛盾、不协调的环节、不稳定及高危因素。比如，明明全世界有超过一半的人拥有智能手机，为什么西联汇款还要在全球设定50万个代理点？⁸埃里克·沃里斯是早期比特币先锋，他常犀利地批评银行系统，他说：“运一个铁砧到中国都要比用银行系统转账到中国快，这真是疯了！钱已经数字化了，你用电汇转账的时候，就不该慢得像在运个盛满钱的菜盘子！”⁹

那么，为什么效率会这么低呢？发明了“生产率悖论”这一术语的经济学家保罗·戴维认为，在现有基础设施中嵌入新技术这种现象，“在过去技术范式转变的历史过程中也常常出现。”¹⁰比如，制造商花了40年时间才从蒸汽动力转变过来，接受了商业电气化，而在他们最终完全采用电气系统前，蒸汽和电气系统常常同时开工。但是在金融系统中，问题就复杂了，因为目前两个技术间还没有出现彻底过渡——现在还有大量遗留技术，有些已经有上百年历史，但是到现在都没有完全尽其所能。

这是为什么呢？其中部分原因是：金融是一种垄断性行业。诺贝尔经济学奖得主约瑟夫·施蒂格利茨曾在一篇评论金融危机的文章中提到：“银行想尽一切办法要提高交易费用。”他认为，就算是零售层面，基本商品和服务的支付“只应该收取1美分的一小部分费用”。“但是你看看他们收了多少？他们要收取成交价的1%-3%甚至更多。有了监管部门和社会的许可，再仗着本身的资本和绝对的规模优势，不同国家的银行都用尽一切办法抽取金融活动中的价值，尤其是在美国，银行业已经赚取了数十亿美元利润。”¹¹从历史角度看，大型的中心化中介机构遇到了无数的机遇。除了传统银行（如美国银行），还有信用卡公司（如Visa）、证券交易所（如纽交所）、票据交换所（如芝加哥商业交易所）、电汇/汇款服务商（如西联汇款）、保险公司（如劳埃德保险公司）、证券律师事务所（如美国世达）、中央银行（如美联储）、资产管理公司（如美国黑石集团）、会计事务所（如德勤）、咨询公司（如埃森哲咨询公司）和大宗商品交易商（如维多石油集团）之类都借势而起，壮大了中介机构的队伍。金融系统的齿轮（指强大的中介机构，他们既有资本又有影响力，通常会实施垄断经济）虽然维持着系统的运作，但是也减缓了其速率，增加了其成本，为自己谋取了大量好处。由于其所拥有的垄断地位，现有机构缺乏动力改善产品、提高效率、优化消费者体验或者去迎合下一代需求的动力。

全球第二古老行业的新面貌

“转基因”金融时代的日子快到头了，因为区块链技术承诺会给未来十年带去翻天覆地的变化，并为那些有能力抓住这个机会的人提供广阔的机会。今天的全球金融产业充满了各种问题：它是过时落后的，是基于数十年前的技术搭建的，这些技术与我们快速进化的数字世界格格不入，使得其运作经常很缓慢和不可靠；它是不包容的，让数十亿的人无法使用基本的金融服务；它是中心化的，让其有数据泄露、其他攻击或完全失败的风险；它是垄断性的，维护现状并扼杀创新。随着创新家和企业家们寻求在这个强大的平台上创造价值的新方法，区块链技术承诺解决这些及更多的问题。

下面列出了六个原因，来解释为什么说区块链技术将深刻地变革金融界，打破金融垄断局面，为个体和机构提供真正的选择权，选择他们创造及管理价值的办法。这一点，全世界的业界参与者都应该重视起来。

鉴证

在金融服务领域，信任协议有着双重含义。互不了解、互不信任的双方，能够达成买卖，这种情况有史以来第一次出现。验证身份、建立信任再也不是金融中介的特权。如果有需要的话，区块链也可以帮助建立信任——根据交易记录、声誉得分（基于总评价得出）以及其他社会经济因素，来验证任意对手方的身份及实力。

成本

在区块链上，网络能够同时兼顾点对点价值转移的清算与结算，并且它会持续工作，所以能够保证账本及时更新。首先，根据西班牙桑坦德银行的数据，如果银行利用这样的技术，预计在不改变基础运营模式

的情况下可以减少200亿美元后台成本。不过实际的数字肯定是更高的。¹²成本锐减后，银行就能为服务匮乏地区的个体和企业，提供更多获取金融服务、市场及资本的机会。任何人在任何地方，打开智能手机，连上互联网，就能进入到全球金融系统的主干道中。

速度

如今，汇款需要3~7天的结算时间，股票交易需要为2~3天的结算时间，而银行贷款交易的结算平均要23天。¹³SWIFT网络每天要处理全球上万家金融机构近1500万笔支付订单，然后要花好几天去进行清算和结算。¹⁴每年在美国处理数万亿美元的自动清算所（ACH）系统也面临同样的情况。不过，比特币网络平均只要10分钟时间就能完成该段时间内所发生交易的清算与结算。而其他的一些区块链网络速度还可以做得更快，诸如比特币闪电网络（Bitcoin Lightning Network）这样的新型创新尝试致力于提高比特币区块链的性能，同时将结算和清算的时间降低到1秒之内。¹⁵旧金山支付公司瑞波实验室首席执行官克里斯·拉森表示：“在往来银行业务中，发送者在一个网络，接受者在另一个网络，这期间不得经过多个账本、多个中介、多个跳跃点，中间的环节真有可能出问题。各种资本需求的规定就是为了应对这个情况。”¹⁶确实，改用即时且无摩擦的价值转移方式，可以释放原来在传输过程中被锁定的资金，不过这一点对那些靠流动资金活力的机构来说就是坏消息了。

风险管理

区块链技术能够降低好几种形式的金融风险。第一种是结算风险，这种风险会让你的交易因为结算过程中出现的一点小故障而被退回。第二种是交易对手方风险，这种风险是指你的对手方在交易结算前违约。最严重的一种风险就是系统风险，它是整个系统中所有未解决的交易对手方风险的总和。维克拉姆·潘迪特把这种风险叫Herstatt风险（取名于

一个无法偿还其债务然后因此倒闭的德国银行），他说：“金融危机中的其中一个风险是，当我与某人进行交易时，我如何知道在另一端他们真的会进行结算？”据维克拉姆·潘迪特表示，区块链上的即时结算能够完全排除这种风险。会计人员任何时候都能及时查看到公司内部运营情况，查看哪些交易正在进行以及网络如何进行记录。交易的不可撤销以及财务报告的即时审核可以消除部分“机构风险”——这种风险是指繁复的书面记录及过久的拖延能让肆无忌惮的管理人员趁机掩盖一些不道德行为。

价值创新

比特币区块链的设计目标是用于比特币的转移而非其他金融资产的处理。但是，这项技术采用开源形式，并且欢迎人们进行各种实验。有的创新家正在开发独立的区块链，将它命名为“竞争币”，用来创建除了比特币支付之外其他用途。而有的人想要利用比特币区块链的规模和流动性，来在侧链上创造“派生”币，这种币可以标上“颜色”来代表任何资产或者债务、（实体或数字的）公司股票或债券、汽油、金条、汽车、汽车付款、应收或应付账款，当然还有货币。侧链是与比特币有着不同特性和功能的区块链，它利用了比特币现成的网络和硬件基础设施，而在安全特性上不会受到影响。侧链通过双向锚定机制与区块链进行相互操作，双向锚定机制是一种在无须涉及第三方交易所的情况下，将资产在区块链内、外进行转移的密码学技术。也有人仍旧在尝试去除货币或代币的元素，在私有区块链上搭建交易平台。金融机构已经开始用区块链技术，进行资产、债务的记录、交换及交易了，最终可能会用这一技术取代传统交易所和中心化的市场，颠覆我们现在对价值的定义和交换方式。

开源

金融服务领域是由遗留系统所构成的技术堆栈，这样的堆栈的高度

几乎有20公里那么高（比喻），现在已经摇摇欲坠了。在这个体系中，改变是一件非常困难的事情，因为每一次改进都必需向后实现兼容性。而区块链作为开源技术，在网络共识的基础上，它能够不断进行革新、反复迭代、完善自身。

这些优点——可鉴证性、减少成本、加快速度、降低风险、创新价值、适应性强——不仅有潜力去转变支付方式，而且也能改变证券行业、投资银行业、会计与审计、风险资本、固定收入以及信用评级机构。

八个核心功能：金融服务领域将如何实现变革

下面是我们认为能够进行突破的八个核心功能，这些在下面的表格中也被归纳出来了。

价值验证

如今我们一般依靠强大的中介机构在金融交易中建立信任并验证身份。要获得银行账户和贷款这种基本金融服务，最终还得靠这些中介的仲裁。区块链可以减少甚至彻底取消某些交易中对这些机构的信任依赖。这项技术也将让节点创建出可供认证、稳健且有着密码学确保安全的身份，并且在需要信任的时候建立信任。

价值转移

每天金融机构都要在全世界范围内转移金钱，并且确保不会出现双重支付的情形：大到数十亿美元的公司间资金转移、资产购置或公司收购，小到iTunes上购买的99美分的歌曲。区块链可以成为任何形式的价值转移的通用标准，范围包括货币、股票、债券及产权等，可以进行大

批量、小批量、近距离及远距离、已知及未知的对手方等形式的交易。因此，区块链对价值转移的意义就像标准化货柜对商品运输的意义一样：这可以极大地减少成本、提高速度、降低摩擦及促进经济增长和繁荣。

价值存储

金融机构是机构、政府和老百姓存放价值的仓库。对普通人来说，银行会把价值储存在保险箱、定期或活期储蓄账户。对大型机构来说，他们需要现成的流动性，并确保有它们的现金等价物能够收到一定的小额回报，也就是所谓的“无风险投资”，比如货币市场资金或国库券。个人不用再把银行作为存放价值的首选或作将其作为定期、活期账户的提供方；而机构则会有一个更加有效的机制来购入并持有无风险的金融资产。

价值贷款

从住房抵押贷款到国库券，可以说金融机构推动了信用证的发行，比如信用卡、抵押贷款、公司债券、市政债券、政府债券以及资产担保的证券。这些贷款业务带动了大量辅助产业的崛起，比如信用检查、信用评分以及信用评级。对个人来说，是信用评分。对机构来说，就是信用评级——从垃圾级别到投资级别。在区块链上，任何人都能直接进行传统债务证书的发行、交易及结算，这样可以减少摩擦、降低风险、提高速度及增加透明度。消费者也能从同行那里获得贷款。这对世界各地的无银行账户人口及企业家来说尤其重要。

价值交换

金钱维持着世界的运转。每天市场要完成全球数万亿的金融资产交换。交易是为投资、投资、套保及套利等目的而进行的资产和金融工具

的买卖行为，其范围包括清算、结算、贮存等交易后处理等环节。区块链能够节省所有交易的结算时间，从几天、几周的周期，缩短到几分、几秒。这种速度和效率为无银行账户人员和未能得到充分金融服务的人员提供参与到财富创造中的机会。

融资与投资

对资产、公司或新企业的投资，为个人带来了获取回报的机会，这些回报会以资本升值、分红、利息、租金或一些组合形式出现。有产业就有市场：在每一个发展阶段，这都能将投资者同企业所有人还有创业人员匹配起来——从天使投资人到上市公司等等。筹资一般需要中间人的参与——比如投资银行家、风投资本家、律师之类。区块链能够实现新形式的点对点融资，它能够提高红利与息票的记录与支付效率，使这些环节更透明、更安全。

价值保险及风险管理

风险管理（保险是其中的一个子集）的目标是保护个体和公司免遭不确定的损失或灾难。更广泛的讲，金融市场的风险管理还推动了一系列衍生产品和其他金融工具的出现，以对冲一些无法预测或无法控制的情况所带来的风险。根据最新计算，所有未偿付的场外交易衍生品的名义总价达600万亿美元。区块链支持去中心化保险模式，使得衍生品在风险管理中的使用更加透明。使用基于个人的社会与经济资本、行为及其他因素为基础的名誉系统，能够使保险公司算出更明确的精算风险，从而在充分了解的前提下做出决定。

价值核算

会计核算是对经济实体金融信息的测量、处理与沟通。这个价值数十亿美元的产业由四大会计事务所掌控着，他们分别是德勤、普华永

道、安永以及毕马威。传统会计实践将无法适应现代金融的复杂程度及操作速率。采用区块链分布式账本技术的核算方式，将使审计与财务申报更及时，而且还能增强其透明度。此外，它还将完善审查功能，从而大大增进监管部门审查公司内部财务行为的能力。

从证券交易所到区块交易所

当Blockstream的奥斯汀·希尔谈及金融产业对区块链技术的兴趣，他表示：“华尔街已经醒来了。”¹⁷比如布莱思·马斯特斯，她是华尔街最具影响力的女性之一，她开创了衍生品产品市场，并将摩根大通商品交易发展成世界巨头。经过一次短期休整后，她以首席执行官的身份加入了纽约初创公司数字资产控股公司。这一决定震惊了很多。她认为区块链会改变她的业务领域，就像互联网改变了其他产业一样，她说：“我会严肃地对待区块链技术，就像20世纪90年代人们对待互联网那样。这是件大事，它将改变金融世界运作方式。”¹⁸

布莱思·马斯特斯之前忽略了很多比特币在早期的故事，这些故事要么就是说比特币被贩毒分子和赌徒利用，要么就是说比特币被致力于创建世界新秩序的自由主义者称赞。这一情况在2014年底出现了变化。布莱思·马斯特斯告诉我们：“有一瞬间我突然明白了什么，然后就开始觉得这一技术对世界的潜在影响或许是积极的。分布式账本技术中的加密程序很有意思，它可能会影响到支付方式，而其基层数据库技术本身则有可能带来更广泛的影响。”¹⁹据布莱思·马斯特斯所言，区块链或能通过“让多方使用相同的信息，而不用反复进行信息复制与对账”来提高效率，减少成本。她认为，作为一个共享的、分布式的及复制式的交易记录，区块是“最佳数据源”。²⁰

“要知道金融服务领域的基础设施，已经有几十年没有更新过了。

前端已经进化过，但是后端还没有。”她说，“这一直是技术投资界的一场军备竞赛，它的目标就是加快交易执行，所以我们可以几纳秒内就测量出竞争优势。可是讽刺的是，交易后的基础设施则完全没有进化。它还是要花好多天，有时还要花好几周来处理交易后进程，包括金融交易的实际结算与记录。”²¹

对区块链技术如此狂热的不止布莱思·马斯特斯一个人。纳斯达克首席执行官鲍勃·格雷菲尔德（Bob Greifeld）说：“我一直坚信，区块链技术能够为金融服务领域的基础设施建设带来根本变化。”²²鲍勃·格雷菲尔德正在通过一个名为纳斯达克Linq的平台将区块链分布式账本技术融入纳斯达克私人股权平台。所有证券交易所都是中心化的市场，而为其带来冲击的时机已经成熟。在2016年1月1日，纳斯达克Linq完成了其首次区块链上的交易。Blockstream的奥斯汀·希尔表示，世界上最大的资产管理机构中的一家公司已经招募了比他们公司还要多的人来投入到其区块链创新工作当中。奥斯汀·希尔的公司共筹得7500万美元并聘用了超过20人。“这些人都明确表示，他们知道如何利用这一技术来改变业务运作的模式。”²³纽约证券交易所、高盛、西班牙桑坦德银行、德勤、加拿大皇家银行、巴克莱银行、瑞银集团以及几乎所有的全球主要金融机构都表达了类似的兴趣。在2015年，整个华尔街对区块链的观点都是积极正面的：在一项调查中，94%的回应认为，区块链技术对金融界有着重要影响。²⁴

表3.1 八个核心功能：金融服务领域将如何实现变革

功能	区块链影响	利益相关人
1. 价值鉴证	可供验证的稳健身份、通过加密保证安全	评级机构、消费者数据分析市场
2. 价值转移——进行资产支付与购买	大小金额的价值转移都不需要通过中介，这样可以大大减少成本，提高支付速度	零售银行业、批发银行业、支付卡网络、转账服务、远程通信、监管部门
3. 价值存储——货币、商品、金融资产都能储存价值。保险箱、定期或活期储蓄账户。货币市场资金或财务票据	支付机制同可依赖的安全存储平台，减少对传统金融服务的需求，定期及活期储蓄账户会变成过去式	零售银行业、支付平台、经纪人、投资银行业、资产管理、远程通信、监管部门

功能	区块链影响	利益相关人
4. 价值贷款——信用卡、抵押贷款、公司债券、市政债券、政府债券、资产支持证券以及其他信用形式	债务可以在区块链上发行、交易与结算，以提高效率，减少摩擦，改善系统风险。消费者可以利用声誉从别人那里获得贷款，这对全世界没有银行账户的人以及创业者来说都非常重要	批发、商业及零售银行，公共财政（即政府财务），小额贷款，众筹，监管部门，信用评级机构，信用评分软件公司
5. 价值交换——投资、套保交易及套利交易。匹配顺序、清算交易、抵押品管理以及估价、结算与保管	区块链把所有交易结算时间从几天、几周，变为几分几秒。这种速度和效率还将为没有银行账户的人及未能得到充分金融服务的人，提供参与到财富创造中去的机会。	投资及批发银行业，外汇交易员，对冲基金、退休基金、零售经纪人，票据交换所，股票、期权、商品交易所——商品经纪人、中央银行、监管部门
6. 对资产、企业及创业进行融资与投资——资本增值、分红、利息、租金或一些组合	点对点融资、企业行为记录的新模型，比如通过智能合约自动支付分红。所有权注册，来自动索取租金以及其他形式收益。	投资银行业、风险投资、法律法规，审计、产权管理、证券交易，众筹、监管部门
7. 价值保险及风险管理——保护资产、房产、生命、健康、营业财产以及商务实践衍生品	借助声誉系统，保险公司将更好的评估保险精算风险，创建去中心化保险市场。并生成更透明的衍生品。	保险、风险管理、批发银行业、股票经纪人、票据交换所、监管部门
8. 价值核算与审计——一种新的公司管理	分布式账本将实现实时审计及财务报告，加快其反馈速度，提高透明度，从而大大改善监管部门审查公司内部财务行为的能力。	审计、资产管理、股东检查人、监管部门

尽管还有其他应用分散了华尔街的注意力，但是对各地金融高管来说，他们的兴趣主要还是全程使用区块链技术安全地处理任何交易，这能够极大地降低成本、提高速度及效率，以及降低业务风险。马斯特斯说：“一笔交易的整个生命周期包括其交易执行、双方之间多次交易的净额结算、交易双方信息及所定条款的核对等，可以在交易提交的层面就发生，这比在主流金融市场里所处的阶段要早得多。”²⁵用鲍勃·格雷菲尔德的话来说就是：“我们目前要花三天时间（T+3）来结算。何不把结算时间改到5~10分钟？”²⁶

华尔街的交易是有风险的，而这项技术能够从物质上减少交易对手方风险以及结算风险，从而降低系统中的系统性风险。世界经济论坛上的金融创新领导人杰西·麦克沃特斯（Jesse McWaters）告诉我们：“最令人激动的就是分布式账本技术的可追踪性，它能帮助我们加强系统的稳定性。”他相信，“这些新的措施，将使监管部门职能的执行更加方便”。²⁷这就是区块链的公共性——透明性、可搜查性，此外，区块链技术的自动结算功能及其不可篡改的时间戳，都能够让监管者了解到事件的变化，甚至还能设置警报以防错过任何细节。

浮士德的区块链契约

银行很少能和透明度联系在一起。大多数金融市场参与者的竞争优势，来自信息的不对称以及比对手方更多的专业知识。但是，比特币区块链所创建的是一种完全透明的系统。对银行来说，这就意味着开诚布公。那么，我们该如何让银行的封闭政策与这样的一个开放平台实现协调呢？

Blockstream的奥斯汀·希尔将这称为华尔街的“浮士德契约”，即一个困难的取舍。²⁸“人们也希望交易可以在几分钟内就完成清算，而不是

等上三天。他们也想立刻知道这是确定完成的以及属实的，”奥斯汀·希尔说道，“但相对应的是，区块链上所有交易都是公开的，这一点让华尔街一些人士感到恐慌。”而解决方案就是在所谓的“许可型”（也被称为私有链）区块链上进行机密交易。比特币区块链完全是“非许可型的”，也就是说任何人都可以访问并实现互动，而“许可型”区块链则要求用户拥有一定的权限，比如要求拥有特定的执照才能在该特定的区块链上运作。奥斯汀·希尔开发了一种技术，可以只让几个利益相关人看到交易的各个部分，同时还能确保其完整性和真实性。

在初步观察下，私有区块链及许可型区块链看上去有一些明显的优势。其中之一是它的成员可以简单地在有需要的时候改变区块链的规则。鉴于在这类模式下交易只需由成员自己进行校验，这样就无须那些耗费大量电力的矿工参与。还有，因为所有的参与方都是可以被信任的，因此不太可能发生51%攻击。由于在大多数情况下节点都是由大型金融机构提供的，因此可以信任所有节点连接的稳定性。还有，它让监管者更容易进行监管。不过，这些优势也带来了弱点。由于规则的改变更容易了，这使得其成员更容易轻视这些规则。私有区块链同时缺乏让技术能快速扩展的网络效应。刻意通过创造新规则的方式来限制特定的自由可能会抑制中立性。最后，由于没有开放的价值创新，这项技术的发展更可能出现停滞并使其容易遭受攻击。²⁹这并非说私有区块链不能得以发展，但金融服务的利益相关方还是必需认真考虑这些方面的担忧。

瑞波实验室（Ripple Labs）已经吸引了银行界大量的关注，并且正在开发其他更聪明的方法来解决这些问题。其首席执行官克里斯·拉森说：“瑞波实验室的目标是做批发银行业务，我们所采用的是一种共识方法而不是工作量证明系统。”这也就说明，任何矿工及匿名节点都不能进行交易的校验。³⁰Chain公司则有一套自己的战略。区块链技术公司Chain从维萨、纳斯达克、花旗集团、第一资本投资集团、金融软件Fiserv公司以及法国Orange电信公司处共筹得3000万美元。它计划开发

企业级区块链解决方案，首要目标就是金融服务领域，在这一领域他们已经同纳斯达克达成了一项协议。区块链技术公司Chain首席执行官亚当·鲁德温认为：“未来所有资产都将是各种各样的区块链上运行的不记名票据”。但它不会变成华尔街习惯了的孤立世界，“因为每个人都会在相同的规格下搭建应用”。³¹或许华尔街会想夺走这一技术，但是这一技术所带来的创新价值并不是他们所能掌控或预测的。

布莱思·马斯特斯也看到了“许可型”区块链的优点。对她而言，需要拥有访问权的，只有少数交易方、销售商、其他对手方以及监管人员。这些被选中的人将会被授予访问权。布莱思·马斯特斯认为，“许可型账本能够为受管制的金融机构减少一些风险，比如和未知方进行交易或者依赖于未知服务供应商（如交易处理商），这些做法从监管角度来说也是不被接受的”。³²这种许可型区块链或“私有链”符合那些在比特币及其相关事项上十分谨慎的传统金融机构会有吸引力。

尽管布莱思·马斯特斯是一家初创公司的首席执行官，但是她的强烈兴趣反映了这个领域内传统金融参与者的更广泛介入。这种对新技术的拥抱越来越反映出一种对科技初创公司也能对高端金融业带来冲击的担忧。对德勤的埃里克·皮斯奇尼来说，“对技术突如其来的兴趣并不是所有人都预料到会发生的”。³³这种热情像传染病一样，正在扩散到世界上规模最大、资历最老的金融机构中。

如今有数十家金融机构在挖掘区块链技术的机遇，而巴克莱银行就是其中之一。根据其首席设计师兼首席数字官德里克·怀特表示，“像区块链这样的技术将会重塑我们的产业”。德里克·怀特正在建立一个开放的创新平台，从而让银行能够与产业内的建设者和思想家互动。他说：“我们非常乐意成为塑造者。不过我们也乐意与技术的塑造者及诠释者联系。”³⁴巴克莱银行削减了几万个传统岗位，然后把资金加倍投入到了这一技术的研究当中，其中最令人瞩目的一项举措，就是发布了巴克莱加速器（Barclays Accelerator）。根据德里克·怀特所言，“我们的队

伍中，30%的公司是区块链或比特币相关公司。区块链是世界从封闭系统转变到开放系统的最重要表现，它将为未来金融服务及其他众多产业带去巨大的影响”。³⁵银行居然在讨论公开系统——我的天哪！

金融公共事业

在2015年秋天，全球九大银行——摩根大通、瑞士信贷、高盛集团、道富银行、瑞银集团、苏格兰皇家银行、西班牙对外银行以及澳洲联邦银行宣布了一项计划，决定共同研究区块链技术通用标准。之后又有21家机构加入，每隔几个月又有一批新的成员加入。³⁶不过这其中还是存在一些问题，例如银行会真地做出行动吗？毕竟，加入这个组织只需要250000美元，不过国际银行区块联盟R3的成立明显标志着产业的向前迈出的一大步。迈克·赫恩于11月加入，他所在的团队还有IBM银行创新项目的前执行架构师理查德·甘道·布朗，以及巴克莱银行前首席工程师詹姆斯·卡莱尔，他目前是R3的首席工程师。³⁷

在2015年12月，Linux基金会与一些大型及一流的公司合作伙伴发起了另一个区块链组织，被称为超级账本计划（Hyper Ledger）。这并非R3的竞争对手；相反，超级账本项目将R3视为其创始成员，其他的创始成员还有埃森哲咨询公司、思科、CLS、德国证券交易所、数字资产控股、美国证券托管结算公司、富士通集团、IC3、IBM、英特尔、摩根大通、伦敦证券交易所集团、三菱UFJ金融集团，道富银行、SWIFT、VMware和富国银行。³⁸这展示出了产业对这个技术的重视程度，但也展示出它们对拥抱比特币这样的完全开放、去中心化区块链的抗拒程度。与R3不同的是，超级账本项目是一个让社区开发“商业区块链”的开源项目。这确实是值得赞赏的，而且也可能会运作得很好。不过要明白一点：这是一个旨在建造限制性技术（如限制网络中节点数量或要求访问权限）的开源项目。在R3的事情上，设立标准是超级账本其

中一个优先处理的事情。该组织的创始成员埃森哲咨询公司的戴维·特里特称，“这个任务的关键是设立可以被产业的参与者使用的标准和共享平台”。

区块链技术还引发了一系列更广泛的公开探讨，包括政府在金融服务领域的监管角色问题。“公共事业”的角色带有天然的垄断性，并由国家高度监管。但因为区块链技术或可减少风险、增加透明度并提高反应速度，于是就一些产业参与者认为技术本身像一个监管机构那样运作。³⁹如果监管部门能够看到银行及市场网络内部的运作情况，那么我们就可以简化甚至去除一些法律法规，对吧？这其实是个很微妙的话题。从一方面看，鉴于极快的创新步伐，监管者将不得不重新考虑他们的监督角色。从另一方面看，过往历史表明政府的缺位经常会让银行做出不诚实的事情。

大型银行是否能够绕开比特币部署区块链并将分布式账本技术的一些元素挑选出来融合到现有的商业模式中，从而掌控主导权呢？有很多迹象表明银行确实朝着这个方向进发，R3只是其中一个标志。在2015年11月19日，高盛集团批准了一项专利，即“利用分布式点对点加密技术来完成金融市场证券结算”，这一技术采用的是一种叫作SETLcoin（结算币）的专有代币。⁴⁰银行将一个原本是送给世界的开源礼物用来申请技术专利，其中的讽刺意味你和我都不应该忘记。也许这就是安德烈亚斯·安东诺普洛斯所害怕的——他曾警告称比特币会从“朋克摇滚转变为轻柔爵士”？⁴¹或者说，银行将要参与到很多不同类别的机构所提供的一流产品和服务的竞争当中，而这些机构的领导者对银行所代表的一切都持反面意见。

未来的金融公共设施要么变成一处四面环墙、修剪整齐的花园，由有权有势的利益相关者所组成的团体控制；要么就变成一个广阔的有机生态系统，在这一系统中，只要有阳光，人们的经济财富就会有丰收。这场辩论还在继续，不过如果我们能从第一代的互联网的经验中获得什

么经验，那就是开源系统要比封闭系统容易扩张。

银行应用软件：零售银行业务中谁才是赢家

“资本界的谷歌”——这就是杰里米·阿莱尔现在正在创建的，也就是“一家消费者金融公司，为消费者提供存款、寄款和收款产品，这些也是零售银行的基础公共设施”。⁴²他认为对任何有上网设备的人来说，这都是一个强大、即时及免费的服务。而他的区块链公司世可国际金融（Circle）就是这一领域规模最大、资本最雄厚的企业之一。

随便你把Circle叫成什么，只要别说它是比特币公司。杰里米·阿莱尔说：“亚马逊不是HTTP（超文本传输协议）公司，谷歌不是SMTP（简单邮件传输协议）公司。Circle也不是比特币公司。我们把比特币视为在经济和社会中使用的下一代互联网基础协议。”⁴³

杰里米·阿莱尔将金融服务视为最后一个堡垒，认为这或许是技术的彻底变革所能获得的最大一个收获。“如果你观察一下零售银行业，它一般有三到四个职能。其一是提供价值贮藏场所，其二是提供支付设施；此外他们还提供信贷并且提供一个能够储藏财富及产生潜在收益的场所。”⁴⁴他的设想是：“在三到五年内，人们可以下载一款应用软件，然后通过数字化方式来贮藏他们需要的任何形式的价值（美元、欧元、日元、人民币及数字货币等）。人们还能即时或近乎即时地完成支付，既能体现全球互操作性，又能确保安全，而且绝不出现隐私泄露问题。最重要的一点，它将会是免费的”。⁴⁵就像互联网改变了信息服务，区块链也将改变金融服务并带来无法想象的各种新能力。

据杰里米·阿莱尔所言，区块链技术的好处包括即时结算、全球可操作性、高安全性以及几乎是免费的交易，无论是个人还是企业都能从中获益。他的计划是让这些服务都能免费提供？世界的银行家们将这称

为异端邪说。当然，高盛和中国风投机构IDG投资5000万美元可不是为了打造一个非营利或公益公司！⁴⁶“如果我们成功建起一家全球特许经营企业，享有几千万用户，这样我们就处于用户交易行为的中心位置，就像是坐在一些很有价值的资产了。”杰里米·阿莱尔希望Circle能拥有“提供其他金融产品的底层能力”。尽管他没有具体提及，但是对其公司而言，数百万客户的金融数据会比他们的金融资产还要值钱。“我们想重新塑造顾客体验及其与金钱之间的关系，并在他们的钱如何被使用及如何能获得资金回报等问题上给予他们选择权。”⁴⁷旧范式的领导者们，你们要注意了。

类似Circle这样的公司并不会受遗留问题及文化的影响。他们全新的策略可以是一个巨大优势。以前许多伟大的创新者都是完完全全的局外人，比如Netflix不是Blockbuster（DVD租赁公司）发明的，iTunes不是Tower Records（唱片公司）开发的，Amazon也不是Barnes & Noble（书店）创建的，你应该明白这个道理了。

Bitpay首席执行官斯蒂芬·佩尔是业界的先行者，他认为新加入的参与者具有一个特有优势。他说：“在区块链上发行股票、债券以及货币这样的可兑换资产，构建必要的基础架构以扩大其规模，并且实现其商业化——这并不需要你有银行从业者的经历。对你而言，你不需要任何传统的基础设施或者机构来创建出如今的华尔街.....你不但可以在区块链上发行这些资产，而且还能创建一套能瞬时完成基本交易的系统。在这一交易中，我可能拥有苹果公司的股票，想从你那里买些东西，然后你想要美元。通过这个平台，我可以提交一个单一的原子化交易（要不交易项目全部完成，要不就全部都不执行），然后使用我的苹果股票给你发送美元。”⁴⁸

真的有那么简单吗？重建金融服务是一场硬仗，但是和万维网前期的电子商务战役还是有区别的。对杰里米·阿莱尔来说，他这样的公司要想扩大规模，就必需加速人类史上最大的一次价值转移，将数万亿美

元从数百家传统银行账户转移到数百万Circle钱包中。这一点并不容易。虽然银行对区块链技术充满热情，但是它们也已经厌倦了这些公司，认为区块链企业就是“高风险”商户。也许，它们这种不情愿是来自对加快自身灭亡的恐惧。在新旧世界的更替中，中介机构如雨后春笋般崛起。加拿大比特币服务公司Vogogo已经同Coinbase、Kraken、Bitpay、Bitstamp及其他公司合作开设银行账户，在符合合规性需求的同时让消费者通过传统支付方式把钱转移到比特币钱包。⁴⁹好吧，这有点讽刺意味。虽然亚马逊轻松超越了现有零售企业，但新范式的领导者也不得处理好与旧范式的领导者的关系。

或许我们需要一位有着硅谷那样乐于实验精神的银行家，而苏雷什·拉马穆尔蒂正符合这个特征。这位出生于印度的前谷歌高管及软件工程师在做出收购堪萨斯州的Wier地区（人口只有650人）的CBW银行时，让很多人都感到惊讶。对他来说，这家小型地区银行就是一个实验室，用于测试区块链协议及基于比特币的汇款通道在跨境汇款中的作用。他的观点认为，如果潜在的区块链企业家并不了解金融服务的微妙差异，那么这些人一定会失败。他说：“他们在为大楼上画窗口，让它看起来既美观又好看，但是 you 无法从外面评估问题。你需要咨询这栋大楼内某个熟悉管道结构的人。”⁵⁰在过去五年里，苏雷什·拉马穆尔蒂一直担任该银行的首席执行官、首席信息官、首席合规官、出纳、门卫及“水管工”。他现在了解银行业的内部运作了。

许多华尔街老兵并不认为这是一场新旧范式的战役。布莱思·马斯特斯认为“对银行来说这种技术对改善效率及华尔街运作水平的机会，与这种技术为新参与者提供的颠覆机会是一样多的”。⁵¹我们不得不感叹，技术的浪潮正在推动一场彻底的变革。为什么三大电视台没有发明YouTube，为什么三大汽车制造商没有开发Uber，为什么三大连锁酒店没有推出Airbnb，这就是原因所在。财富1000高管层在追求新的发展道路时，新手们已经在速度、敏捷度以及产品上超越了他们。不管谁是第

一，这场势不可挡的技术变革，与难以撼动的金融服务（世界上最根深蒂固的产业）之间的摩擦一定会逐渐升级。

商业界的“谷歌翻译”：会计核算及公司管理的新框架

Subledger是会计行业的一家初创公司，其首席执行官汤姆·莫宁尼说：“会计就像蘑菇——它们长在阴暗处，靠粪便提供营养。”⁵²会计学被称为金融学的语言，除了专业人士，常人很难弄懂。如果每一笔交易都能在一个共享的全球分布式账本上进行，那我们还用得着公共会计师帮我们翻译这些内容吗？

现代会计行业源于15世纪的一位意大利人卢卡·帕吉奥里的好奇之心。他看似很简单的发明就是复式记账法，即在每一笔交易都会给交易双方带来影响，每一方必需要在资产负债表(记录公司资产和负债的账本)上各自记录一笔借项和一笔贷项。卢卡·帕吉奥里通过编写这些规则，制定出了一种秩序，如果没有这一秩序而是随意混乱的运作，那么就有可能阻碍企业规模的扩张。

罗纳德·科斯认为会计就像邪教组织。当他还是伦敦经济学院的学生时，他就把记账行为看作“宗教的一种表现形式”。“委托给会计师保存的这些账簿就是圣书”。会计专业学生认为他的挑战是“亵渎神灵”⁵³他怎么敢质疑他们的“那些计算折旧、估算库存、分配成本之类的记账方法，根据这些方法所得出的结果虽然都不相同，但都是能被全盘接受的会计实践活动”。此外还有一些其他类似的行为，至少是被视为完全“不值得尊敬的”。所以汤姆·莫宁尼绝对不是第一个跳出来批评这个职业的人。

现代会计工作有四个问题。首先，当前的体制是靠管理人员发誓他们的账本没有问题。但是，包括美国安然、美国国际集团、雷曼兄弟、

世界通信、美国泰科以及日本东芝在内的好几十起知名案例表明并非所有管理者都能做到诚信。贪婪蒙蔽了人类的双眼，滥用亲信、贪污腐败以及虚假报告不仅导致了企业破产、民众失业和市场崩溃，还会增加了资本成本并对股权相关业务也带来不利影响。[54](#)

第二，AccountingWeb的研究表明，人为出错是会计问题的主要原因。很多时候，问题都从某人错误地用他的胖手指（打比方）在电子表格中输入的一个数据开始，然后就像蝴蝶效应一样，一个小问题变成大问题，其影响会涉及各个财务报表中的不同计算结果。据28%的专业人士汇报，人们曾在它们公司的企业系统中录入了不正确的数据。[55](#)

第三，奥克斯利法案（Sarbanes-Oxley）这样的新规则对阻止会计舞弊行为并没有太大的帮助。公司复杂程度的增加、交易涉及的方面更广及现代商业的速度让隐藏错误的行为变得更简单了。

第四，传统记账方法不能与新型商业模式协调。以小额交易为例，很多审计软件都能够进行两位小数的处理（如精确到1美分），这对任何形式的小微支付来说意义都不大。

会计学（财务信息的测量、处理与沟通）本身不是问题。它在当今的经济中扮演着重要角色。但是，会计方法的实施必需与现代的要求匹配。在卢卡·帕吉奥里的时代，每天都要进行账目审查。而如今，是每月或每个季度进行一次。你很难找出另一个产业是经历了500年的技术进步却将完成一个任务所需时间增加了9000%的。[56](#)

世界账本

如今，公司会记录每一笔交易的借项和贷项，因为这里有两个输入项，所以是复式记账法。在世界账本中，他们可以轻松加上第三个输入

项，并且让需要进行检查的人——包括公司股东、审计人员及监管者即时访问账本。可以设想一下，当一家像苹果公司这样的大型企业要出售产品、采购原材料、支付员工薪资、或者在资产负债表上记录资产及债务情况时，世界账本会记录该交易并在区块链上发布一个时间戳凭证。公司的财务报表将会变成一种活化的分类账本，具有可审计性、可搜索性以及可验证性。对财务报表进行及时更新就像电子表格功能一样简单，只要点击一个按键，就会生成一份不可改变的、完整且可供搜索的财务报表，并且不会出错。公司或许不想让所有人都看到这些数据，因此高管可以只将访问权限交给监管者、管理人员以及其他重要的利益相关者。

业内许多人都看到了世界账本对会计工作的内在影响。巴克莱银行的西蒙·泰勒认为，这种账本可以满足监管部门的合规要求并且降低风险，他说：“我们做的很多监管汇报都是在重复将我们所做的事重新说一遍，毕竟所有记录都在系统内部，没有其他人可以看到。”⁵⁷世界账本以及任何事物的透明记录意味着“监管者可以访问到相同的数据基础层。这也就意味着，工作内容会减少，成本会降低，而我们每一秒都需要对所产生的财务记录负责。这一点非常厉害”。⁵⁸对Circle公司的杰里米·阿莱尔来说，监管部门受益最多。他表示：“银行检查人员一直都是在靠不透明的、私人控制的专有账本以及财务记账系统来执行职能，即‘记录账目’。而通过共享的公共账本，审计人员和银行检查人员可以通过自动的审查来检查资产负债表的基本健康状况及公司的实力。这是一个强大的创新成果，能够使监管、审计以及会计核算的部分环节实现自动化”。⁵⁹

它将诚信融入系统里了。基于以太坊的三式记账法初创公司Balance3的克里斯汀·伦德奎斯特说：“所有诈骗的实施将变得异常困难。你要想作弊就得持续进行，无法在中途改变过去的记录。”⁶⁰奥斯汀·希尔认为：“这是一个不停地进行审计和验证的公共账本，意味着你不

需要信任合作伙伴的账本；报表或交易日志已经将诚信的因素融入进去了，因为网络本身也在进行验证。这就像是一种持续地以密码学方式实现的先验审计。你不需要依赖普华永道或者德勤，也不会存在对手方风险。如果账本说这个记录是真的，那么它就是真的”。⁶¹

德勤是世界四大会计事务所之一，它一直在尝试了解区块链技术的影响。埃里克·皮斯奇尼是德勤加密货币中心的负责人，他告诉客户区块链“会给你的业务模式带去很大风险，因为目前银行业务就是去管理风险。如果有一天这个风险消失了，那么银行还能做什么”？⁶²另一个会受到颠覆的是审计业务，而审计业务占据了德勤收入的三分之一。⁶³埃里克·皮斯奇尼说：“这是对我们自己的商业模式的一种颠覆，对吗？如今我们花大量时间去审计公司，并且根据所花费的时间进行收费。可是在未来，如果这个流程因为区块链的一个时间戳就完全简化了，那么我们的审计方式也会发生改变。⁶⁴或者这会彻底消灭所有的审计公司？”

德勤开发了一套名为PermaRec（永久记录的英文缩写）的解决方案。“通过PermaRec，德勤会将这些交易记录到区块链上，然后就快速地对交易一方或双方进行审计，因为所有的交易都被记录下来了。⁶⁵但是，如果区块链上的第三个输入项是自动地进行时间戳验证并能够让所有人查看的，那么任何人在任何地方都可以决定账目是否平衡。相反，德勤及其他三大审计事务所发展最快的领域是咨询服务。许多客户已经开始关注区块链。这样的慌乱恰好提供了机遇，创造了转移到咨询业务价值链条的机会。

汤姆·莫宁尼是一位大胆的企业家，他把自己描述为“永恒的乐观主义者”，他把周期性会计核算同这个现象联系了起来：“看着人们在闪光灯下跳舞，你知道他们是在跳舞，但是你看不清楚细节是什么。也就是看起来很有意思，但是很难理解其中每一个步伐。”⁶⁶周期性会计核算会

产生一个快照。而审计的定义就是一个回顾过去的过程。就是在回顾这个过程。要想通过周期性财务报表来呈现完整的公司财务健康情况，就像是把一块牛肉饼还原成一头牛一样。

根据汤姆·莫宁尼所言，大多数大型公司绝不会想要一个放置在公共领域的透明会计记录，他们甚至不愿意让拥有特殊权限的人（如审计人员或监管者）能够轻易地来访问这些记录。一家公司的财务情况是保密程度最高的秘密之一。此外，许多公司希望其管理层能够在一些特定项目的会计方法上保留一定程度的灵活性，像如何识别收入、资产折旧或者记录一笔商誉减值费用等。

但是，汤姆·莫宁尼相信，公司会从更高的透明度中得到好处，这不仅是其财务部门运作的或审计成本的降低，还能带来公司市场价值的增加。他表示“第一家采用这一体系的上市公司将能看到股价或市盈率方面的明显优势，而在其他公司，投资者还得焦虑地等待每季度财务信息如挤牙膏般地公开”。汤姆·莫宁尼说：“如果有公司能每时每刻告诉你所有信息，谁还会去投资那些一季度才公开一次的公司呢？”⁶⁷

投资者将会要求公司使用三式记账法来满足其治理标准吗？这个问题并不是牵强附会的。许多机构投资者，如加州公务员退休系统已经制定了一套严格的公司治理标准，并且不能在这些标准未能满足的情况下对某公司进行投资。⁶⁸三式记账法可能就是下一个这样的标准了。

三式记账法：隐私保护是为了个人而非企业

也有对三式记账法持怀疑态度的人。伊莎贝拉·卡明斯卡是《金融时报》的记者，她认为三式记账法会使越来越多的交易在资产负债表外进行，“总是会有人不遵守协议的，他们会躲起来，在平行的离线网络中隐藏秘密的价值，这些离线网络也就是我们所说的黑市、资产负债表

外资产及影子银行”。[69](#)

一个人应该如何处理不基于交易的会计手段（特别是在无形资产的认定问题上）？我们应该如何追踪知识产权、品牌价值甚至是名人的状态？这可以联想到汤姆·汉克斯，在区块链影响他的品牌价值前，这位奥斯卡影帝得接多少烂片？

关于三式记账法的争论并不是对传统会计方式的否认。在某些领域，我们还是需要有能力的审计人员的。但是，如果三式记账法能够通过实时精确性、可验证的交易记录及即时审计而极大地提高透明度以及响应能力的话，那么区块链就能解决会计工作的很多大问题。德勤需要有人对无形资产进行实时评估，并且执行其他区块链做不到的会计职能，这样它就不需要派遣过多的审计人员了。

最后，我们真的如此渴望能有一个不可篡改的记录来录入所有东西吗？在欧洲，法院赞成人们“有权被忘记”，来回应人们关于清除互联网历史痕迹的请愿。那么同样的规则是否适用于公司呢？答案是否。为什么Uber司机要根据消费者满意程度来获得评分，而公司高管就不需要这样做？我们来设想这样一个机制，可以将它称为信任软件，可以在公共账本上汇报反馈意见并保持一个独立的、可搜索的成绩，用于记录公司的诚信记录。在公司内部的黑盒子中，阳光（公开）是最好的消毒剂。

三式记账法是众多区块链创新中，第一个与公司治理相关的创新。就像社会中许多机构样，我们的公司也在忍受各种合法性危机。罗伯特·蒙克是股东维权人士，他认为“资本主义已经变成‘高层统治’，受高管们的控制并且为高管们的财富利益服务。我把这些人叫作‘管理界的国王’”。[70](#)

区块链将权力归还给股东。假设有一个代币可以用于代表某种资产的权利，比如“比特股份”（bitshare），它们会和一个选票或多个选票绑定，每个都标有颜色来代表某个特定的公司决策。人们可以即时从各地

投票选出自己的代理人，从而使公司主要行动的投票过程变得更具有响应性、更具有包容性，而且被操纵的可能性更低。公司内部的决定将需要达到真正的共识，并且在产业范围内实施多重签名方案，在这种情况下，每位股东都拥有一把通向公司未来的钥匙。一旦票数统计出来，最终决定的内容以及董事会会议纪要都会被标上时间戳，记录在一个不可篡改的账本中。

公司应该有权改变历史，或选择被人们遗忘吗？[71](#)答案是不。作为社会中的人工产物，公司的运营执照附带着特定的责任。实际上对社会而言，公司也有义务公开所任交易信息。当然，公司有权利和义务来保护商业机密以及员工、人员及其他利益相关者的隐私。但是，这和隐私保护又有所不同。对各地的管理人员来说，透明度的增加是一个重要的机遇：通过拥抱区块链，支撑最高标准的公司治理规则，并作为公司领导者担当维系信任的职责。

声誉：你就是你的信用分数

无论你是申请第一张信用卡，还是想要贷款，银行在乎的就是一个数据：你的信用分数。这个数字的作用是反映你的信贷价值及违约风险。它是一系列输入项的集合，从你所借时限到支付记录。大部分零售信用就是根据这个来考察。但是这种计算方式也有深层问题。其一，它的范围太狭隘。一个年轻人并没有信用记录，但是也许他声誉不错，也能有完成承诺的良好记录，或者他有一个富有的伯母。这些因素都没有算进信用评分中。其二，这种分数制可能会使个人萌生不正当的动机。现在越来越多的人使用借记卡，即现金卡。因为他们没有信用分数，就收到了这样的“处罚”。然而信用卡公司会鼓励那些没有收入来源的人去申请信用卡。其三，分数变动常常滞后：数据输入项经常会过时，相关度也很低。在一个人20岁时出现的延时还款与其50岁时的信用风险基本

上没有太大的关联性。

FICO是一家美国公司，之前叫Fair Isaac Co，一直在美国信用评分市场上处于领先地位，但是其分析忽略了大部分相关信息。马克·安德森表示“贝宝可以根据你的易趣购买记录，在几毫秒内完成实时信用评分——这种信息来源比用于生成你的FICO信用评分的信息要好多”了。⁷²这些因素与区块链技术生成的交易、数据及其他属性结合到一起，能够实现一种更稳健的算法，用于发放信贷并规避风险。

你的声誉是什么呢？我们每个人都至少有一个声誉。对于业务及日常生活的信任来说，声誉非常重要。迄今为止，金融中介机构还没有用声誉作为在个人和银行之间建立信任关系的基础。假设有一位小型企业的所有者想要申请一笔贷款，通常情况下，信贷人员会根据个人档案（身份的一个方面）及其信用分数来决定是否发放贷款。当然，人类的信息不仅仅是社保编号、生日、主要居所和信用历史等。但是，无论你是可靠的员工、活跃的志愿者或热心的市民，或是你家小孩所在足球队的教练，银行既不会知道，也不会关心。信贷人员可能会欣赏你的诚信，但是银行评分系统不会。由于目前社会和经济系统正在构建中，所以这些声誉因素很难用公式去表示，也很难存为文档或投入使用。这些因素都很难量化或被记录下来。

有数十亿人除了在他们的直接社交圈外没有任何声誉记录，那么他们怎么办呢？虽然有些穷困地区也有金融服务，但是很多人连身份证明这个必要的门槛都跨不过去，这些证明包括身份证、居住证或者金融历史等。这在发达国家也是一个问题。在2015年12月，很多大型的美国银行拒绝了将新印制的纽约身份卡作为开启银行的有效证件，而不顾已经有超过67万的人申请了证件，也不顾银行的联邦监管者们已经批准了其用途。⁷³而区块链可以解决这个问题，它根据人们的各种属性以及之前的交易记录，来授予人们一种在传统银行系统之上的新的替代选项。

此外还有很多用例(尤其是信用方面),在这些用例中,区块链能够在需要信任元素的各方之间建立信任关系。区块链技术不仅能确保贷款资金进入借款人账户,而且可以保证借款人按照一定利息归还借款。它利用双方自己的数据来给双方赋予好处及加强他们的隐私,并根据某人过去在区块链上的经济活动及社会资本等因素,来为其建立长期有效的经济身份。帕特里克·迪根是身份识别初创公司个人黑盒子的首席技术官,他说:“个人总有一天能设置并管理自己的身份,并和其他对等网络及节点建立可靠的连接。”而这一切都得益于区块链技术。⁷⁴因为区块链会在一个不可篡改的记录中登记及储存所有交易,每一笔交易都能给声誉和信贷评估积分增加分数。此外,个人能够决定以何种角色同哪个机构进行沟通。帕特里克·迪根表示:“我能创造出不同身份,代表我的每一面,然后我可以选择某个身份来和该公司进行沟通”。⁷⁵区块链上的银行及其他公司要求采集的信息不能多于他们提供服务所需的信息。

这个模式经验证是有效果的。BTCJam是一个点对点贷款平台,它以声誉为提供信贷的依据。用户可以将BTCJam上的个人资料同Facebook、领英、易趣或者Coinbase账号关联起来,从而增加声誉考察的深度并丰富其信息。朋友也能通过Facebook按照个人意愿进行推荐。你甚至可以提交真实信用分数作为属性之一。这些私人信息都不会对外公开。用户可以在平台上以较低信用分数起步,但通过证明自己是一个可靠的借用人就可以很快建立声誉。最佳战略是以“声誉贷款”起头,来证明自己的可靠。作为用户,在融资过程中,你必需回答投资人的问题。若忽视这些问题就会让人们产生警惕,而社区也会犹豫要不要资助你。有了第一笔贷款(从一个可以负担的数额开始)后就要按时还款了。如果你按时还款了,那么你的分数就增加,而且社区其他成员也有可能给你一个好评。截止到2015年9月,BTCJam已经放出了18000笔贷款,总额超过1400万美元。⁷⁶

企业家埃里克·沃里斯呼吁大家进行更多尝试,“通过这种基于声誉

的系统，那些更可能负担得起一套房子的人，或许能轻松购入第二套。然而对那些不太可能做到这一点的人来说应当会更难获得贷款”。对他而言，这套措施“会降低那些表现良好的参与者的成本，而增加表现不好的参与者的成本，这是正确的激励机制”。⁷⁷在声誉系统中，你的信贷额度并不是根据FICO评分，而是根据一系列构成你的身份的属性并能表明你偿还贷款能力的集合信息来决定的。公司的信用评级方式也将改变，从而反映由区块链带来的新信息及见解。如果有这么一种工具，能够累积声誉并追踪不同方面的声誉信息，比如金融可信度、职业能力及社会意识等；如果设想能够根据共同的价值观来获得信贷，即贷款给你的人同时欣赏你在社区中的角色及你的目标。

区块链IPO（首次公开募股）

2015年8月17日所处那一周，是糟糕的一周：标准普尔500指数创下四年来最差数据，各地的金融专业都在谈论世界经济发展的减速，以及潜在的危机。传统的首次公开募股被市场撤出，并购进程因此停滞，硅谷也开始因它们估值过高的独角兽企业而感到坐立不安。独角兽企业是指估值超过10亿美元的私有公司。

在这场“厮杀”中，一家叫作Augur的企业发动了有史以来最成功众筹项目之一。在首周，有超过3500位来自美国、中国、日本、法国、德国、西班牙、英国、韩国、西班牙、南非、肯尼亚以及乌干达等地的投资人总共贡献出了400万美元。整个过程没有中介、投资银行、证交所、必要的申报文件、监管部门以及律师，甚至没有Kickstarter或IndieGoGo这种众筹网站的参与。女士们、先生们，欢迎来到区块链首次公开募股的时代。

将投资者与企业匹配起来的功能是金融服务产业可能被颠覆的8大功能中的一个。自从20世纪30年代以来，股权融资的途径（通过私募发

行、首次公开募股、二级发行以及上市后私募投资）一直没有出现过太大的变化。[78](#)

多亏了新型众筹平台的存在，一些小型公司也得以使用互联网获得资金支持。Oculus Rift以及Pebble Watch就是早期这一模型的成功案例。然而，参与者并不是直接购买股票。如今，美国创业企业融资法案允许小型投资人直接投资众筹项目，但是投资人及创业者还是需要通过Kickstarter或者IndieGoGo这样的平台，以及传统支付方式（比典型例子是信用卡及贝宝）来参与投资。中介机构能够最终裁决每个细节，包括归属权。

区块链的首次公开募股增进了人们对这一概念的理解。现在，公司能够通过区块链上发行代币、加密证券（代表公司里的某种价值）的方式筹集资金。它们能够代表股权或债券，或者在Augur的案例中就是做市商的席位，让所有者有权决定平台将开放哪些预测市场。以太坊是一个比Augur还要成功的例子，它通过众售其原生代币（以太币）资助了一个全新区块链项目的开发。今天，以太坊是市值排行第二、增长速度最快的公共区块链。Augur众筹平均投资额是750美元，当然也可以想象下可以将最低参与额度设置成1美元甚至10美分。世界上任何人，无论他多穷，所处地区多偏远，他都可以成为股票市场投资者。

在线零售商Overstock正发起的计划或许是最具雄心壮志的加密证券计划，其超前思考的创始人帕特里克·伯恩相信区块链“可以为资本市场做的事就正如互联网为消费者做的事那样”。这个名为Medici的项目让公司可以在区块链上发行证券，最近得到了美国证券交易委员会的批准。[79](#)这个公司开始发行其首批基于区块链的证券，如一个由FNY资本附属机构在2015年发行的价值500万美元的加密债券。[80](#)Overstock声称很多金融服务机构和其他公司正排着队等待使用这个平台。确实，得到来自美国证券交易委员会的默许让Overstock在一个将会很长的旅程中有了先发优势。

如果区块链首次公开募股的吸引力继续增加，它们最终将颠覆全球金融系统中的很多种角色（包括股票经纪人、投资银行人员以及证券律师），并且改变投资的本质。我们希望，通过将区块链的首次公开募股整合到新的价值交换平台上，比如Circle、Coinbase（资金最充足的比特币交易所初创公司）、Smartwallet（全球各种有价资产交易平台）以及其他新兴公司，我们预期一个分布式的虚拟交易所会诞生。旧范式的“护卫们”也在表达关注。纽约证券交易所投资了Coinbase，而纳斯达克正在把区块链技术整合到其私有市场中。纳斯达克首席执行官鲍勃·格雷菲尔德从小处做起，希望利用区块链技术“来精简财务记录，减少成本，同时提高精确度。”⁸¹不过，纳斯达克和其他现有的参与者显然有更大的计划。

预测市场的市场

Augur正在创建一个去中心化预测市场平台，这个平台会奖励正确预测未来事件的用户——包括体育赛事、大选结果、新产品的发布、名人后代的性别等等。它是如何运作的？Augur用户可以买入或卖出在一个未来事件结果中对应的股份，其价值是对某个事件发生概率的预测。因此，如果比率打平（也就是50对50），那么每股的购入价就是50美分。

Augur依靠的是“群众的智慧”，这是一种科学原理，即由很多人组成的群体对未来事件预测的结果总是会比一两个专家预测的结果还要准确。⁸²也就是说，Augur将市场精神作用于预测的准确性上。之前也有过几个中心化的预测市场，比如好莱坞股票交易所、Intrade以及HedgeStreet（现在的Nadex），但是这其中的大多数都因为监管及法律问题被关闭或走向失败。

使用分布式区块链技术，可以使系统在出现故障时更容易恢复，也

能更加准确且有效对抗崩溃、出错、关闭、流动性等问题，以及团队委婉所言的“老套的辖区监管。”Augur平台上的仲裁者就是裁判，他们的合法性来源于其声誉分。做正确的事情——比如正确的陈述事件发生原委、体育赛事或大选结果就能得到更多声誉分。维护系统的诚信还能带来其他金钱利益：你的声誉分越高，你就可以有更多的市场，这样你就能收取更多的费用。用Augur的话来说，“我们的预测市场消除了对手方风险及中心化服务器，通过比特币、以太币及其他稳定的加密货币来建立全球市场。所有资金都存储在智能合约上，没有人可以盗走钱财”。⁸³Augur通过对犯罪实行零容忍政策来解决各种不道德的合约发行。

对Augur领导团队而言，人类的想象力是预测市场效用的实际极限。在Augur平台上，任何人都能发布一个对任何事物的预测（有着明确的定义），并加上明确的结束日期——从琐碎的事件，比如“布拉德皮特和安吉丽娜朱莉会离婚吗”到重要的大事，比如“2017年6月1日欧盟会不会解体”。这对金融服务领域、对投资者、经济参与者以及整个市场的影响都是巨大的。设想一下，在尼加拉瓜或肯尼亚有一位农民，他没有可靠的工具来应对货币风险、政治风险或者天气及气候变化；而如果他进入预测市场，那么就可以对冲干旱或其他灾难的风险。比如，他可以购买一份预测合约，预测粮食产量会低于某一数据或者国家降雨量低于预期等，这样当条件满足时他就能收到付款。

预测市场能够满足一些投资者对某一特定事件结果的下注需求，比如“本季度IBM的每股收益会超过至少10美分吗”？如今，对公司收益的“预估”报告，大多出自几个所谓专业分析师所预测的均值或中位数。通过众人的智慧，我们对未来的预测可以更加现实，从而实现更高效的市场。预测市场能够作为全球不确定因素以及“黑天鹅”事件的对冲工具：“希腊经济今年会缩水15%以上吗”？⁸⁴我们现在常常依靠少数几个人的评论来发出警报，而预测市场将更加公平地为全球投资者提供一个早期警告系统。

预测市场能够补足并最终转变金融系统的许多方面。设想一下关于公司行为结果的预测市场——包括收益报告、合并、收购以及管理层的变更等。预测市场可以为保险价值及风险的对冲提供更多信息，甚至还可能替换深奥难懂的金融工具（比如期权、掉期以及信用违约掉期）。

当然，不是所有事件都需要一个预测市场。需要有足够多的人来增加其流动性，从而吸引众人。尽管如此，这一市场都有着巨大的潜能与机遇，并且所有人都可以参与其中。

八个核心功能之路线图

区块链技术将影响金融服务领域的方方面面——从零售银行业和资本市场，到会计和监管。它还将促使我们重新思考银行和金融机构在社会中扮演的角色。安德烈亚斯·安东诺普洛斯说：“比特币没有对金融机构的紧急救援、银行假期、货币管制、资产冻结、提取限制以及银行营业时间。”⁸⁵

旧世界是层级化的，它发展缓慢、不愿改变、封闭又不透明，而且由强大的中介机构进行控制；而新秩序会相对平等一些，它会提供点对点解决方案，加强隐私与安全，并且做到更透明、更包容及更具创新性。可以肯定的是，未来一定会出现混乱和冲击，但是这也是一个让产业的领导者今天就可以做些事情的绝佳机会。金融服务产业将会在未来的几年间有出现和增长的可能性；随着中介数量的减少，更多的产品和服务就可能以更低的成本提供给更多的人。这是一件好事。关于许可型、封闭式区块链能否在去中心化世界立足，还有待讨论。曾经资助过SecondMarket，如今是数字货币集团首席执行官的巴里·西尔伯特表示：“对于现有大型金融企业所提的一些观点，我有些怀疑。当你手里只有锤子的时候，你就会觉得所有东西都是钉子。”⁸⁶我们相信，区块链技术正以不可阻挡的力量，为根深蒂固的、受监管的及僵化的现代金融

基础设施带来冲击。[87](#)它们的碰撞将会改变未来几十年金融领域的发展。我们希望，金融这一领域能够从工业时代的金钱机器转型为一个实现繁荣的平台。

第四章 重新设计公司的架构：核心与边缘

打造共识系统®公司

2015年的7月30日是全球范围内的一群程序员、投资者、企业家和企业战略家的一个重要日子——这群人认为以太坊是对商业甚至是文明的重大变革。以太坊经过了18个月的开发过程，在那天上线了。

在第一个以太坊软件开发公司（Consensus Systems共识系统®）的布鲁克林区的办公室里，我们率先见证了以太坊的发布。大约在早上的11:45，随着以太坊网络创建了它的“创世块”，到处都是人们击掌庆祝的声音，之后，大量的矿工们开始进行算力的竞赛，试图赢得第一个区块里的以太币——这是以太坊的货币。那天实在令人异常紧张。一阵特大暴雨的到来让东部河区域受到了影响，每一个人的智能手机上的紧急洪水警报声此起彼伏。

根据其网站的介绍，以太坊是一个运行去中心化应用（也就是智能合约）的平台。“系统会严格执行这些合约，而且这个系统并不会有故障时间、审查、诈骗或来自第三方干扰等因素的影响”。以太坊系统中的以太币（Ether）用于激励网络中的节点以实现交易的验证、网络安全的保护，以及就系统中“存在什么，发生过什么事”这个问题达成共识，这一点是有点像比特币的。不过与比特币不同的是，以太坊自带强大的开发工具，能够帮助开发者及其他人创建软件服务。这些软件服务的范围非常广泛，从去中心化游戏到股票市场都有所涉猎。

以太坊的概念最早是在2013年由维塔利克·布特因提出来的，他是

一名俄裔加拿大人，当时才19岁。他曾经跟比特币的核心开发者争论，认为比特币平台需要一个更加强大的脚本语言，专门用于应用程序的开发。当比特币核心开发者拒绝了他的提议后，他决定创建自己的平台。可以说，ConsenSys是最早的一个尝试，公司成立的目的是为了创建基于以太坊的应用程序。若要找一下历史上的例子做比喻的话，下面这个比喻是很明显的：维塔利克·布特因之于以太坊，就如同林纳斯·托瓦兹之于Linux系统一样。

当讨论到有关区块链及以太坊技术兴起的话题时，ConsenSys的联合创始人约瑟夫·卢宾说：“有一点对我来说已经很明显了，那就是我们应该联合起来，为这个破碎的经济和社会建造新的解决方案，而不是让大家继续浪费时间在大街上张贴各种海报。”¹不要去占领华尔街了，直接发明属于我们自己的华尔街吧。

就如很多企业家一样，约瑟夫·卢宾有一个大胆的理想，他不仅仅要建造一个伟大的公司，还要解决世界的问题。他平静地说，该公司是“一个区块链相关的制作工作室，旨在搭建去中心化应用程序（大部分是在以太坊上的）”。这种描述是很低调的。不过，若ConsenSys在搭建的应用程序真的能得到实施和应用，将会有可能对现有的体系带来冲击，并为数十个产业带来深远的影响。这些项目包括一个分布式的三式记账会计系统；一个去中心化版本的Reddit（Reddit是一个非常流行的论坛，其中心化的管理机制让其饱受争议）；一个为自主执行合约（又叫智能合约）而设的档案构造与管理系统；为商业、运动和娱乐业而设的预测市场；一个公开的能源市场；一个旨在与Apple和Spotify竞争的分布式音乐模式，不过，其实这两家公司也能使用这个应用程序²；以及一个为大规模协作、创作工作及扁平化架构的公司进行群体治理的一整套业务工具套件。

这个关于ConsenSys的故事，并不是与其在基于区块链的产品或服务上的雄心壮志有关，而是关于他们培育自己的公司的努力以及他们按

照全体共治的思想在开拓管理科学的重要新领域。全体共治是一种协作方式，用自组织的架构取代了传统体系中的定义、分配工作的分层规划过程。“我目前并不想照搬现有的全体共治体系，我感觉它太僵硬了，架构化也很明显。不过，我们正试图将它的很多理念整合到我们的架构和流程中。”约瑟夫·卢宾说道。这些理念包括“采用动态的角色分配，而不是传统的固定职衔；分布式的，而不是委任的权力；透明化的规则，而不是办公室政治；快速的叠架而不是大规模地重构”，这些描述都适用于区块链的工作机制。ConsenSys的组织架构、创造价值的方式以及它管理自身的方法不仅与产业公司是不同的，与典型的网络公司也是不一样的。

约瑟夫·卢宾并不是一个理想主义者，更不是一个无政府主义者或自由主义者，这与加密货币运动里面的一些人不太一样。不过他确实认为若我们想资本主义继续存活下去，就必须继续做出改进，特别是舍弃那种基于“命令与控制”的层级化结构。他认为这种架构是不适用于这个由网络连通的世界的。他注意到即使在今天，大型的网络将世界连接在一起，让我们的沟通变得更廉价了，但层级化的结构还是存在的。比特币是与此结构相反的，“这是一个由全球人民组成的社会，可以在10分钟（甚至是10秒）内就发生的事实达成共识并做出决定。这显然为实现一个更有自主权的社会提供了机会。”他说道。人们的参与程度越高，繁荣的程度也就越高。

这是管理者角色的终结，但管理任务长存

ConsenSys是按照一个由所有的雇员（“成员”）开发、改进、投票后最终采用的计划进行运作的。与层级化架构不同的是，约瑟夫·卢宾将ConsenSys的这种架构定义为一个“枢纽”，而其中的每一个项目就像是一个“车轮上的辐条”一样，主要的贡献者会拥有其中的权益。

在大多数的情况下，ConsenSys的成员可以选择工作的任务，并没

有自上而下的任务。约瑟夫·卢宾说道，“我们尽可能地进行资源的共享，这包括软件部件的共享。我们组建小而敏捷的团队，但它们之间是有协作的。我们有不少即时的、开放的和丰富的沟通交流。”成员们选择在2-5个项目中工作。当其中一个人看到某项工作需要完成，他或她就会投入进去，根据他们的适合担任的角色或多或少地驱动其往一个有价值的方向发展。“我们经常讨论各种事情，所以人们对很多可能会被推动向前的事情都有一定了解，”他说。不过这些事情经常在变化。“敏捷意味着你需要动态调整你的优先级。”

约瑟夫·卢宾并不是老板。他在运营中的主要角色是顾问。“在很多情况下，人们请教我或其他人有关选择工作方向的事情。”他说。在Slack³及Github⁴这样的协作平台上，他暗示他们可能选择的方向包括“建造我们希望实现的服务和平台（甚至包括一些我们目前还不了解的）”。

成员的所有权明确地对这种行为做出激励。每一个人会直接或间接地拥有每一个项目的一部分：以太坊平台发行的代币，成员可以将其交换成以太币并转换到任何其他货币。“我们的目标是在自主性和相互依存之间达到一个良好的平衡”，约瑟夫·卢宾说道。“我们将自己视为紧密协作的企业家角色的集体。在某个阶段，可能需要表明真的需要完成某个事情了，如果没有人挺身而出揽下这个工作，那么就要为了这个角色先招聘一些人，或鼓励内部的人员去负责这件事”，约瑟夫·卢宾说道。不过，总体来说，“每一个人都是能够自我管理的成年人。我刚才有提到我们经常沟通吗？然后我们就做出自己的决定”。

这里面最适合的标语是敏捷、开放和共识：先识别出需要完成的工作，在热切并有能力完成该任务的人群中分发工作量，并就他们的角色、责任、补偿等问题达成共识，然后将这些权利归纳成“明确的、细节的、清晰的、自我执行的协议，可以作为我们关系中所有的商业角度相关事项的黏合剂”，他说道。一些协议是根据绩效进行支付的，而其

他的一些会用以太坊的方式分配在年薪中，而其他的一些更像是带有与项目相关赏金的“寻求参与”，这些赏金会取决于项目完成的程度，如书写一行代码。如果代码通过了测试，则该赏金就会自动被释放。“所有的事情都能在台面上进行，而且是足够透明的。激励机制是明确的、可细分的”，他说道，“这让我们更自由地进行沟通，拥有创新意识，并根据这些预期适应情况的变化。”

我们可否造一个新词，区块链公司(blockcom)，即一个在区块链技术上建造和运行的公司？这就是我们的目标，即在以太坊平台上运行实现更多的像ConsenSys这样的公司，范围包括治理、日常运营、项目管理、软件开发和测试、雇佣和外包、补偿和资助。区块链同时也支持声誉系统，成员可以为每一个人作为协作者的表现评分，这样就能实现社区中的信任联盟。约瑟夫·卢宾说道，“永久存在的数字身份、人格及声誉系统会让我们更诚实，彼此之间行有更良好的行为”。

这些能力都让一个公司的边界变得模糊了。这其中并没有成立公司的默认选项。ConsenSys生态系统的成员们可以通过就战略、架构、资本、表现和治理达成共识并创建自己的分支项目。他们可以创建一个现有市场上进行竞争的公司，或为一个新的市场提供基础设施。当公司发起后，他们可以改变这些设定。

企业的去中心化

区块链会为世界各地的公司减少摩擦。“更低的摩擦意味着更低的费用，因为有价值中介的价格是通过去中心化自由市场这种最高效的价格发现机制决定的。现有的市场参与者再也不能利用法律、监管、信息和权力的不对称性而在作为中介的角色中从交易里抽取过高的价值，甚至比他们提供的价值都高。”约瑟夫·卢宾说道。

ConsenSys有可能建造某种真正去中心化的自治组织吗？这种组织将会由其非人类的价值创造者拥有和控制，通过智能合约而不是人类的

中介去管理吗？“全程都可以！”约瑟夫·卢宾说道，“这是一个运行在去中心化的全球计算底层的大规模智力集合，其中的人类或软件参与者可以各自执行其特定任务，也可以在自由市场中进行合作和竞争，这样的大型协作可以改变公司的架构”。为满足持续的客户需求（如实用性和维护），一些参与者可能需要在更长的时间段里留任；其他的一些人将会聚集起来去解决短期的问题，问题解决后就可以解散了。

如果用激进的去中心化和自动化流程移除人类参与者在决策制定中的参与度，这样会有风险吗（如失控的算法）？“我对机器智能并没有太大的担忧。我们将会与其一起进化，而且在可遇见的将来它将会为人类服务。它可能会在我们之上进化，不过那是没问题的。”他说道，“如果是那样的话，它会占据生态位里的一个微小的位置。它会以不同的速度、不同的相关时间尺度运作。在那样的情况下，人工智能与人类、一块石头或地质变迁的过程并不会区分开来。我们已经进化到很多物种之上了；这些物种有很多还生存得不错（在它们当前的形态下）”。

ConsenSys还是一个小型的公司。它的宏伟实验或许不能成功。不过它的故事提供了公司架构的巨变过程的一个视角，这个巨变可能帮助释放创新的动力，并利用人类资本的力量为财富的创造及繁荣服务。区块链技术带来了新型的经济组织及新的价值组合。一些分布式的公司模式正呈现出来——所有权、架构、运作、奖励和治理——这远远超出了鼓励创新、员工激励和集体行动的范畴了。这些东西或许就是实现一个更繁荣、更包容经济体长久所需的先决条件。

商业领袖们有机会对组织价值创造的问题进行重新思考。他们可以在区块链上商议、起草和执行协议；与供应商、顾客、雇员、承包商和自治的代理人无缝衔接；而且，他们还可以公开由这些代理人所组成的团队，让其他人都能看到，这些代理人也可以将他们的价值链中的过剩能力出租或授权出去。

改变公司的边界

在互联网发展的第一个时代，管理学思想家们（唐塔普斯科特也是其中之一）赞扬了网络化的企业、扁平化的公司、开放创新和商业生态系统，他们认为这些模式将取代工业化模式下的层级制度。不过，20世纪早期的公司架构基本上还是维持原状。即使是大型的网络公司也与杰夫·贝索斯、马里萨·迈耶、马克·扎克伯格等名义领袖一起采用了从上至下的架构。因此，这些现有的机构——特别是一些依靠人们的数据营利并以不透明的方式进行运作的机构，一些在频繁的数据泄露事件发生后却无须承担太大责任的机构，他们有什么理由希望使用区块链技术去将权力分散出去，提高透明度，尊重用户隐私和匿名性，并将那些财富远少于他们正在服务的用户的群体包容进来呢？

公司的交易成本与架构

我们先从一些经济学知识开始。在1995年，唐塔普斯科特使用了诺贝尔经济学奖得主罗纳德·科斯的理论去解释互联网将会如何改变公司的架构。在他1937年写的《公司的本质》这篇论文中，罗纳德·科斯提出了经济里面的三种成本：搜索的成本（寻找创造某种事物所需要的所有正确信息、人员和资源）；协调（使得这些人进行高效的协作）；以及签订合约（为生产中的每一个活动进行人力和物力成本的谈判，保管商业机密及监管、执行这些协议）。他假设一个公司的规模会不断扩大，直到在公司内执行某项交易的成本大于在公司外执行该项交易的成本。⁵

唐塔普斯科特认为互联网可以在一定程度上降低公司内部的交易成本；不过我们当时想，因为互联网可以在全世界范围内访问，因此它会降低整体经济的成本，最终降低人们进入经济体系的障碍。是的，互联网通过浏览器和万维网的确降低了搜索的成本。它通过电子邮件、ERP这类数据处理应用程序、社交媒体和云计算等技术降低了协调方面的成

本。很多公司从顾客服务和会计的外包业务中受益。市场营销人员可以直接与顾客交流，甚至将顾客转换为生产者（专业消费者，prosumers）。产品规划人员将创新的任务众包出去。生产商也受益于大型的供应网络。

不过，令人惊讶的现实是，互联网对公司架构的冲击并不明显。资本主义为人所知的基础依然是工业时代的层级化架构。网络确实让一些公司将生产流程外包到低成本的地区中。不过互联网也降低了公司内部的业务成本。

从层级制度到垄断

今天的公司仍旧保存着层级化的架构，大部分的活动都是在公司内发生的。管理者们依然将自己视为组织人才、无形资产（品牌、知识产权、知识和文化）及激励员工的良好模式。公司的董事会依然给公司高管和首席执行官们发放过高的报酬，远超于他们所创造价值的合理量度。这并不是一个偶然的現象，产业结构还是在持续地创造财富，而不是繁荣。实际上，就如我们指出的那样，权利和财富越来越高地集中在大型企业当中，这方面的证据已经很明显了。

另一名诺贝尔奖得主奥利弗·威廉森也做出过同样的预测，⁶并指出了这种现象对生产力的负面影响：“我们足可以观察到，从自主供应（通过小型公司的集合实现）到（在一个大型公司里的）统一的所有权这个趋势是无可避免地伴随着激励的强度（在一体化的公司里激励会更弱）及管理控制（控制更广泛）这两个方面的改变”。⁷Paypal的联合创始人彼得·蒂尔在他那本可读性极强、争议性极高的书《从0到1》赞颂了垄断机制。作为一个兰德·保罗的支持者，彼得·蒂尔称“竞争是为失败者们而设的.....具有创造力的垄断体不仅对社会的其他方面是有益的；它们也是一个能让社会变得更好的强大引擎”。⁸

彼得·蒂尔或许对努力成为某个产业或市场的支配者这种行为的看法是对的，但他并没有证明垄断对顾客或社会整体是有利的。恰恰相反的是，在大多数民主化资本主义国家的竞争法体系是从一个相反的结论中衍生出来的。公平竞争的理念可以追溯到罗马时代，那时候触发某些条例可能会遭受到死刑的惩罚。⁹当公司没有真正的竞争对手时，他们的增长速度可以是非常慢的，在公司内外抬高价格。即使在技术产业里，很多人认为垄断或许可以在短期内促进创新，但在长期会给社会带来危害。公司或许能通过为顾客提供他们喜欢的酷炫的产品和服务积累垄断优势，但这个蜜月期最终是会结束的。与其说他们的创新成果不再令人满意，倒不如说这些公司自身开始走向僵化。

大多数思想家意识到创新通常来自公司的边缘部门，而不是核心部门。耶鲁大学法学教授尤查·本科勒也认同这一点：“垄断势力或许有很多的资金能投入到研发当中，但通常不会为创新所需的纯粹、开放的探索这种内部文化投入。互联网并不是来自垄断当中，而是来自边缘。Google并不是来源于微软。推特并不是来源于AT&T，更不是来源于Facebook”。¹⁰在垄断体制下，官僚主义的层级使得位于高层的高管们与市场信号和边缘位置的新兴技术隔离开来了，而在这些边缘位置里，各个公司在彼此之间、其他市场、其他产业、其他地区、其他知识学科及其他世代之间展开竞争。约翰·哈格尔和约翰·西利·布朗认为，“现在，创新潜力最高的地方是全球商业环境的外围位置，忽略这一点的话后果自负”。¹¹

高管们应该为区块链技术感到兴奋，因为从边缘位置发起的创新潮流或许是前所未有的。举例来说，从主要的加密货币（比特币、黑币、达世币、未来币、瑞波币）到主要的区块链平台——为点对点众筹而设的Lighthouse项目、作为分布式登记处的“公证通”（Factom）、作为去中心化信息发送系统的Gems、作为去中心化应用程序的MaidSafe、作为分布式云的Storj以及作为去中心化投票机制的Tezos，下一个时代的

互联网将会有真实的价值附加在上面，并为参与者提供真实的激励。这些平台有望保护用户的身份，尊重用户的隐私权等权利，确保网络运行的安全性，降低交易成本，这样即使是无法获得银行服务的人群也可以参与进来。

与现有的大公司不同的是，他们不需要用品牌来彰显其可信性。通过将它们的源代码免费公开，并与网络中的每一个参与者分享权力，使用共识机制以确保正直性，并在区块链上公开地运行业务，这些技术为那些梦想破灭和被剥削的人群带来了新的曙光。因此，区块链技术还是提供了一种可靠的、高效的方法，不仅能消除中介成本，还能极大地降低交易成本，将公司变成网络，将经济权力分散开去，最终促进财富的创造和塑造一个更繁荣的未来。

1.搜索成本——我们如何寻找新的人才和新的顾客？

我们该如何寻找所需的人员和信息？在我们寻求将市场的资源用在公司内部运作时，我们该如何判断他们的服务、商品和能力是否是最好的？

虽然公司的架构基本上保持不变，但互联网的第一个时代极大地降低了这些方面的成本，并促进了一些重要的改变。各种业务的外包只是一个开始。通过使用创意集市（Ideagoras，一种交易创意的公开市场），像宝洁这样的公司正寻找有资质的人们对产品或流程进行创新。事实上，宝洁公司的60%的创新成果是来自于公司之外的，即通过搭建或利用像Innocentive或Inno360这样的创意集市实现。而像加拿大黄金公司这样的公司已经提出了一个公开挑战，在全球范围内寻找最聪明的头脑去解决它们最难的问题。加拿大黄金公司将其地质数据和知识在公司范围外公开发表，从而发现了价值34亿美元的黄金，使得该公司的市值翻了一百倍。

现在，想象一下若拥有对万维账本（World Wide Ledger），即一个存储了世界上大部分结构化信息的数据库的搜索能力，会带来什么新的机会？谁将某个发现成果转卖给了谁？价格如何？谁拥有这个知识产权？谁有能力处理这个项目？医院的员工有什么医学技能？这场手术是谁主刀的，结果如何？这个公司存下了多少碳排放额度？哪个供应商有中国市场的经验？哪个承包商会根据它们的智能合约及时交货，而且不超出其预算？这些问题的结果将不会是简历、广告链接或其他推送出来的内容；它们将会是交易历史、个人和公司可证明的业绩，并通过声誉度进行排序。这个场景你明白了吗？以太坊区块链的创始人维塔利克·布特因说道：“区块链将会降低搜索成本，将问题分解，让你能够拥有平行化聚合和垂直化聚合的机构组成的市场。这是前所未有的。现在，你有了一个能执行所有事情的工具。”¹²

现在，有几个公司正在搭建为区块链而设的搜索引擎，这显然是与其中潜藏的机会有关的。Google的愿景是对世界上的所有信息整理。考虑到这个新兴的平台有可能包含世界上的所有信息，Google已经调派了不少的人员进行调查。

互联网的搜索和区块链的搜索还是有一些明显的差异。首先是用户的隐私权。在区块链上，虽然交易是透明的，但用户对个人的数据有控制权，并可以决定将这些数据用在哪些方面。他们可以匿名地参与进来，至少是以伪匿名（通过假名实现的匿名）或部分的匿名性的方式进行参与。若用户决定公开某些信息，其他有兴趣获取这些信息的参与者就能进行搜索。区块链理论家安德烈亚斯·安东诺普洛斯称“若你想实现匿名交易，还是可以做到的……不过区块链对透明性的支持比对匿名性的支持更显著”。¹³

很多公司都需要对招聘流程进行重新的思考和设计。例如，人力资源或雇员管理人员将需要学习如何用区块链进行是/否问题的查询：你是人类吗？你有一个应用数学的博士学位吗？你能用Scrypt、Python、

Java或C++写程序吗？你从1月开始到明年6月能全职工作吗？以及其他
的资质。这些查询将会在招聘市场上寻找人们的信息并给出符合条件的
名单。他们也可以让预期中的人才将他们相关的专业信息放在区块链上
并给予一定的报酬，这样就能用于查询了。人力资源部门的人员必需掌
握声誉系统的用法，在不需要获取与职位无关的信息（年龄、性别、种
族、祖国）时就能与该人进行互动。他们也需要一个能够在不同维度的
开放性之间能够自由切换的搜索引擎（从全面的隐私保护到全面的信息
公开之间）。它能够终结来自潜意识的甚至制度上的偏见，移除猎头公
司或高管招聘的费用。若要找一個不利的因素，那就是精确的查询会带
来精确的结果。意外发现某种人才的机会将会变得越来越小——在以
前，这种人才可能缺乏相关的资质，但学习能力非常强，也能为公司带
来急需的创造性成果。在新的技术下，这样的人才可能就难以被发掘出
来了。

这在市场营销中也有类似的情况。公司可能需要付费获取潜在顾客
的“黑盒子”以读取他们的信息，并决定这个顾客是否能成为公司的目标
受众。这个顾客可能会在全局状态下隐藏特定的信息（如性别），毕竟
即使是一个“不是”的答案也是很有价值的。不过这种做法会让公司在查
询时无法了解“是或否”答案之外的信息。首席营销官和营销机构将需要
重新考虑任何基于邮件、社交媒体和移动终端的市场营销方式：基础设
施或许会将沟通的成本降低到0，但顾客将会要求提高相应的费用以补
偿阅读公司信息所浪费的时间。换句话说，你需要付费给客户才能让他
们了解你的推销信息，不过你可以对查询过程进行量身定制（只面对特
定的受众），这样就能在无须侵犯隐私的情况下精确地将信息送达到你
的目标受众中。在新产品研发的每一步，你可以用不同的查询进行测
试，了解不同的微小受众市场。我们可以将它称为“黑盒子营销”。

另一个区别就是搜索可以是多维度的。当你今天在万维网上搜索
时，你会及时地搜索到一个快照，这个快照是在过去的几个星期内进行
索引的。¹⁴计算机理论家安东诺普洛斯将这种现象称为二维搜索：水平

化（在网络范围内进行广泛的搜索）和垂直化（对某个特定的网站进行深度的搜索）。第三个维度是顺序，以观察信息上传的先后次序。“区块链可以增加时间这个额外的维度，”他说道。用三维的方式对曾经发生的所有事的记录进行搜索，这具有非常深远的意义。为了证明这一点，安东诺普洛斯在比特币的区块链上进行搜索，发现了那个著名的（也是首个）商业交易记录——一个名为拉斯洛的人用10000个比特币购买了两个比萨。“区块链提供了一个几乎是考古学一般的记录、一个深度的发掘结果，能够永久地保存信息。”（为了省去你计算所花费的时间，若那个比萨的价格是5美元，而那时候1美元能购买2500个比特币，那么截至行文之时，这个比萨的代价已经有350万美元的价值了.....不过这已经偏题了。）

对公司来说，这意味着需要有更好的判断力：管理者们需要雇用那些已经展示出有良好判断力的人才，因为错误的决定带来的后果无法再回撤了，也无法操控事件发生的顺序，无法对某个高管声名狼藉的行为做出抵赖。对那些非常重要的决定来说，公司需要实施内部的共识机制，所有的股东都需要就某个项目涉及的关键问题进行投票，以免到时候他们都以“我之前不知道这事”的态度来抵赖。或者，可以使用预测市场去测试各种场景。如果你是未来的安然公司的高管，你就无法推卸责任了。对新泽西州的州长克里斯·克里斯蒂来说，就不太可能在这种情况下对检察官声称自己不知道任何关闭乔治·华盛顿大桥的计划。

第三个区别是在价值方面的：互联网上的信息非常多，不太可靠，而且是可以销毁的；而区块链上的信息是稀缺的、不可篡改的及永久保存的。安东诺普洛斯对最后的这个特性是这样描述的：“如果有足够的经济激励实现区块链的长期保存，则它持续数十年、数百年甚至数千年的可能性不可低估”。

这是一个神奇的概念。区块链作为一个像考古学意义上的记录，就如同亚述和美索不达米亚的古老石板那样。纸质的记录是短暂的、容易

灭失的，而（具有讽刺意味的是）最古老的信息记录形式的石板，则是最具持久的。可以想象它在公司的架构中将会带来的影响。想象一下若有一个永久的、可搜索的重要历史信息的数据库，就如金融的历史一样。公司负责填写如下材料（财务报表、年度报告、给政府或捐赠者填写的报告、为潜在雇员/客户/顾客设计的营销材料）的人员可以从这个公开的、不可篡改的公司视角开始执行他们的工作，甚至增加一些过滤层，让股东可以简单地查看所需的数据。公司也可以有交易相关的行情显示系统和指示板，一些是用于内部的管理流程，一些是用于公开的。这一点是肯定的：你的所有竞争对手将会把这些数据源和指示板作为他们的竞争对手研究项目。那么，你为何不将这些信息放到网站上，让所有人都访问你的网站呢？

这让公司更有动力去在公司之外寻找资源，这样他们对候选对象的质量和记录都能有更多的了解，不论这些对象是个人还是公司。

像ConsenSys这样的公司正在开发身份系统，让职位的候选人或候选承包商可以编写自己的个人形象，以向雇主透露相关的信息。它无法以中心化数据库那样的方式被入侵。用户有动力给自己的个人形象贡献数据，因为他们拥有并能控制这个形象，其隐私保护是可以进行配置的，而且能利用自己的数据实现经济利益。这是与像领英（LinkedIn）这样的公司不一样的，领英是一个由大公司拥有、实现经济价值但并没有实现彻底安全性的中心化数据库。

罗纳德·科斯和奥利弗·威廉森之前有可能想象到有一种平台能将搜索的成本降低，从而让公司可以在自身以外寻找耗费更低、绩效更好的资源吗？

2.签约成本——我们究竟同意做什么？

我们如何与其他人达成协议或签订合约？降低公司所需人才或资源的搜索成本只是第一步，但这远远不足以让公司出现明显的改变。所有

的参与方都必需就协作的问题达成一致。公司存在的第二个原因是合约上的成本，如价格商议、确定功能、描述供应商货物或服务的条件、监管并执行条款相关的成本，以及在一方违约时采取的补救措施。

我们一直都有某种社会契约以及对专门的角色关系的理解，如部落里的一些人负责打猎并保护部落，而另一些人将部落集中起来并提供庇护。实时的物物交换从人类文明发端时起就存在了。合约则是更为近代的事情，从那时开始我们开始交易“承诺”而不只是财产了。口头的协议已经被证明是很容易被操纵或记错的，目击证人也是不可靠的。怀疑和互不信任阻碍了陌生人之间的协作。合约需要立即填写，除了外部的强制力外，合约本身并没有强制条款执行的正式机制。书面的合约是一种归纳义务、建立信任和树立期望的方式。书面合约在某人无法信守承诺或意外发生的情况下提供指引作用。但这些作用都无法在真空中存在，这必需依赖于一个认可合约和执行每一方权利的法律框架。

今天，大多数合约还是由原子（纸张）而不是数位（软件）构成的。因此，它们有极大的局限性，通常只用于记录某项协议。就如我们可能看到的那样，如果合约具有软件的性质（在区块链上的智能、分布式的存在），那么其可能性将会是无限的，而不仅仅会让公司更容易地与外部资源进行协作。可以想象一下，若《美国统一商法典》是在区块链上实现的，那影响会是怎样？

罗纳德·科斯和他的接班人们声称在公司内签订合约的成本要比在外部的市场上低很多，即一个公司实质上是为创建长期合约而设的媒介，这是因为签订短期合约所需的成本太高了。

奥利弗·威廉森进一步阐述了这个想法。他认为，公司存在的目的是解决冲突（主要是通过在公司内的各个参与方签订合约）。在公开市场上，法庭是唯一的纷争处理机制，它的成本很高，耗费时间，而且经常无法得到令人满意的结果。还有，他认为在诸如诈骗、其他非法活动或利益冲突的例子中，根本就不存在市场纷争处理机制。“事实上，内

部机构的‘合同法’是具有宽容性的，这一点让公司就成为组织内部的上诉法庭。这也是公司能够行使市场无法达成的命令的原因。”¹⁵奥利弗·威廉森将公司看成是一个为契约安排而设的“治理架构”。他认为组织架构对降低管理交易的成本是有意义的，还有“依赖于合约而不是选择，时常会让我们对复杂经济组织的理解变得更深入”。¹⁶这在对经济组织的学习过程中是一个经常出现的场景，迈克尔·詹森和威廉·梅克林这两位经济学家将这个问题解释得非常到位。他们认为机构实体只是由一堆合约和关系所构成的集合。¹⁷

今天，一些博学的区块链思想家们已经认真思考这个观点。以太坊的创始人维塔利克·布特因认为公司的代理人（如高管）只能在经过如董事会这样的机构批准后才能将公司资产用在特定的用途，而董事会这类机构又要向股东负责。“如果一个公司做了某件事情，那是因为董事会同意这个事情应该做。如果一个公司雇用了员工，那这意味着此雇员同意在特定规则集合下（特别是涉及报酬的事项）为公司的顾客提供服务，”维塔利克·布特因写道。“有限责任公司意味着特定的人群在行事时能够降低对来自政府的法律诉讼的担忧，即一群人行事时享用比个人单独行事时更多的权利，不过他们最终还是人。无论如何，这还是由人和合约构成的。”¹⁸

通过降低合约成本，区块链让公司更开放，并在公司边界之外发展新的关系，这就是区块链可以实现的事情。以ConsenSys为例，它可以在不同的成员集合之间构造复杂的关系，一些是在公司内的，一些是在公司外的，一些处于中间的状态。智能合约代替传统的管理者对这些关系进行管理。成员们自己安排到项目上，定义好所认同的可交付成果，并在交付成果后得到报酬——这一切都在区块链上完成。

(1) 智能合约

这个世界变化的速率正为智能合约设下舞台。越来越多的人不

仅“能使用计算机”，还“能熟练地使用计算机”。就如交易活动展示出来的迹象一样，这个新的数字中介与其纸质形态的前任的属性有着显著的差异。就如密码学家尼克·绍博指出的那样，它们不仅能够获取更大范围的信息（如非语言性的传感器数据），而且是动态的：它们能够发送信息并执行特定的决定。就如尼克·绍博说的那样，“数字媒体能够执行计算、直接操作机器并以远高于人类效率的方式进行推理”。[19](#)

出于本文讨论的目的，我们将智能合约定义为是一种能够为个人和机构之间的协议提供保护、实施、结算执行的计算机程序。因此，它们可以在商讨和定义这些协议的时候提供帮助。尼克·绍博在1994年提出了这个概念，而那年第一个网页浏览器网景（Netscape）也在市场上推出了：

“智能合约是一个用计算机处理的交易协议，能够执行合约的条款。智能合约的主要目的是为了满足不同合同条件（如支付条款、扣押权、保密性甚至是执行），减少因恶意行为或意外带来的争议，并减少对可信任的第三方中介的依赖。相关的经济目标包括降低因诈骗而导致的损失、仲裁和执行成本以及其他交易成本。” [20](#)

那时候，智能合约只是一个概念，因为当时的技术无法实现尼克·绍博提到的这种特性。那时候有类似电子数据交换（EDI）这样的标准格式，可以在买家和卖家的电脑之间传输结构化的数据，但并没有真正能够触发支付及金钱换手的技術。

比特币和区块链可以改变这些事情。现在，交易各方可以达成协议，当他们满足协议规定的条款时就能自动地进行比特币的交换。更简单的例子是，你的姐（妹）夫也无法抵赖在曲棍球赛事上参与的赌注了。有个没那么简单的例子是，当你购买了一个股票，交易可以即时结算，而股份能及时转让给你。还有，当承包商提交了满足特定规格的软

件时，他们就能得到报酬。

用于执行功能有限的智能合约的技术手段已经存在一段时间了。合约是经过商议的一个交易，而且在交易开始前就具有效力。安德烈亚斯·安东诺普洛斯用一个简单的例子进行了解释：“如果我和你现在同意我将会为你桌面上的那支笔付款50美元，这完全是一个有效力的合约。我们可以说，‘我承诺我会付50美元购买你桌上的那支笔，’而你的回应是，‘是的，我愿意接受。’这样的结果就是法律上的‘要约、承诺和对价。’我们已经达成了一个协议，而且可以在法院里执行。这与我们所做出的承诺的技术实施方案是无关的”。

对安德烈亚斯·安东诺普洛斯来说，区块链之所以吸引他的兴趣，原因是我们能够在这个内置了结算系统的去中心化技术环境中履行各种金融义务。“这是非常酷的”，他说，“因为我现在可以真的为了这支笔付款给你，你可以马上看到这些钱，然后你将这支笔放到邮件中，我可以进行验证。这显然增加了我们做生意的机会。”

法律专业产业正慢慢地接触这个机会。就如每一个处于中间位置的人一样，律师也可能受到去中介化的影响，最终需要适应这个趋势。智能合约研究这样的专长可能是那些想引领合同法创新的律师事务所的重大机会。不过，法律产业并不是以探索新领域著称的。法律专家（也是一个关于区块链的新书的共同作者）亚伦·赖特告诉我们，“律师们的反应是很慢的。”²¹

(2) 多重签名：智能的复杂合约

不过，或许你会说智能合约的复杂性和耗时的商议过程所带来的成本超出了公开边界所能带来的好处？现在看来，并不是这样的。若合作伙伴能够事前决定一个协议的条款，那么其监视、执行和结算成本将会极大地降低，甚至可能完全免除。还有，结算可以实时发生，甚至全天都能在几微秒的时间内完成（取决于具体的交易）。更重要的是，通

过与更高级的人才展开合作，公司可以实现更好的创新成果，提高自身竞争力。

我们来考虑一下使用独立承包商的案例。在数字化交易的早期，区块链只适合用于最简单的双方交易。例如，若艾丽斯（Alice）需要一个能快速帮她完成代码的人，她可以很快地在一个合适的讨论区以匿名的方式发布一条“需要程序员”的信息，然后鲍勃（Bob）就能看到这条信息。²²若价格和时间点都合适，鲍勃就会发送一些以前的工作成果案例。如果他的案例满足艾丽斯的需求，艾丽斯就会出价。他们同意如下的条款：艾丽斯会立刻发放一半的费用，而剩下的一半费用在代码接收完并成功测试后才会发放。

他们之间的合约是很简单的，包含了一个雇佣的要约及接受该工作的答复，而且不需要用书面的方式写出来，不过他们在区块链上的互动还是使得这些条款被记录下来了。他们对比特币的所有权是与数字地址关联起来的（一长串字符），这个地址有两个部件：作为地址的公钥和有权访问该地址的任何代币的私钥。鲍勃将他的公钥发给艾丽斯，然后艾丽斯将款项汇到这个地址中。网络将该次转账记录下来了，并将那些比特币与Bob的公钥钱包关联起来。

如果这时候鲍勃决定他不想完成这个项目呢？在这个双方的交易中，艾丽斯并没有太多的选项。她无法让她的信用卡公司撤销这笔交易。她（还）不能到民事法庭并对鲍勃提出合同违约诉讼。除了一个随机生成的字母数字代码及一个在线的广告，她无法得知鲍勃的身份，除非鲍勃在一个中心化的平台发布了可用于追踪其身份的广告，或他们通过一个中心化的服务交换了邮件。她倒是可以表明鲍勃的公钥是不能再被信任的，因此降低了他作为程序员的声誉度。

若无法信任其他人执行区块链外的交易，这个交易有点像囚徒困境了：它还是需要一定程度的信任。声誉度系统可以在一定程度上缓和这

个不确定性。不过我们需要往这个匿名和开放的系统中引入信任 and 安全性。

在2012年，“比特币核心开发者”加文·安德烈森往比特币协议中引入了一类新的比特币地址，名为“pay to script hash, P2SH。”它的目的是让一方“注资实现仲裁形式的交易，无论这交易的复杂程度如何”。²³各方使用多重认证签名或秘钥而不是单一的私钥去完成一个交易。社区通常将这个多重签名特性简写为“miltisig”。

在多重签名交易中，各方就以下两个问题达成共识：生成了多少把钥匙（N），以及需要多少把钥匙（M）才能完成一个交易。这就叫M/N签名计划（安全协议）。想象一个带锁的箱子，你需要多把物理钥匙才能打开。通过这个特性，鲍勃和艾丽斯可以事先委托一个中立的、利益无关的第三方仲裁者帮助他们完成交易。这三方中的每一方都会持有1/3个私钥，要访问转账后的资金就需要有任意两个私钥的签名。艾丽斯会将她的比特币发送到一个公开地址。这时，这些资金可以被任何人查看，不过没人可以访问。当鲍勃看到这些资金已经被发送过来了，他就履行自己的合约义务。若验收的时候艾丽斯认为鲍勃的商品或服务是无法令人满意的，而且她感觉受到欺骗了，这时她可以拒绝给鲍勃提供第二把钥匙。这两方将会求助于仲裁者（第三把钥匙的持有者），以帮助他们解决争议。仲裁者只在争议发生后进行干预，在任何情况下他们自己都无法接触到这些资金，因为这是一个由智能合约实现的机制。

若要远程签订合约甚至是自动化签订合约，你需要在一定程度上信任系统会根据协议实现你的权利。如果你不能相信另一方，你就必需相信争议解决机制以及（或）其后的法律体系。多重签名技术使得那些刻意保持公正的第三方能在匿名交易中引入安全性和信任。

多重签名技术越来越流行了。一个名为Hedgy的初创公司正使用多重签名技术创建期货合约：各方就一个将来交易的比特币价格达成共

识，只交换其差价。Hedgy从来不持有抵押品。各方在执行日之前将抵押品放置到一个多重签名的钱包中。Hedgy的目标是将多重签名作为智能合约（完全自执行，验证透明化）使用的基础。²⁴可以将区块链视为是在匿名性和开放性之间的辩证产物，而多重签名能够平衡这两个方面的需求。

另外，智能合约能够改变人力资源主管的角色。人力资源部门需要明白人才在公司内外都是存在的。使用智能合约以降低与外部资源建立关系的成本，这是他们需要应对的一个挑战。

3. 协调成本——我们应该如何协同工作？

假设你已经找到了合适的人才，也建立了相应的联系。那么，你该如何管理他们呢？罗纳德·科斯在他的文章中时常提及协调、匹配和规划不同的人、产品和流程以实现一个高效地创造价值的企业及这些工作所涉及的成本。与那些认为公司内部是有着内部市场的经济学家不同的是，罗纳德·科斯认为“若一个工人从A部门转移到B部门，他转移的原因并不是因为价格的相对改变，而是因为他接到了命令”。²⁵换句话说，市场通过价格机制调配资源，而公司通过权威的命令调配资源。

奥利弗·威廉森继续进行了阐释，他认为有两种较为显著的协调系统。第一种（市场机制）是在去中心化的资源及其相关需求和机会调剂过程中的价格机制。而第二种（传统机制）是“公司采用一种不同的原则，即层级化——通常是用权力去影响资源调剂”。在过去数十年，层级化机制一直备受争议，人们认为它在扼杀创新、降低主动性、降低人力资本的价值，及通过不透明的运作机制推卸责任。有一点是确定的，很多层级化的体系最后变成了生产力低下的官僚主义体系。不过，虽然层级化这个概念的口碑很差，但作为层级化体系最有力的拥护者之一，生于加拿大的心理学家埃利奥特·雅克（Elliot Jacques）在1990年的《哈佛商业评论》的一篇经典文章里说道，“经过35年的研究，我认为管理

体系的层级化对大型机构来说是最高效、最坚强、实际上也是最自然的架构。若有合适的架构，层级化可以释放能量和生产力，使生产力合理化，并鼓舞士气”。[26](#)

问题就在这里，在近代的商业历史中，很多层级化的体系效率并不高，甚至令人啼笑皆非。重要证据是《呆伯特法则》（*Dilbert Principle*），这是史上销量最高的管理学书籍，作者是斯科特·亚当斯。下面这段对话是摘自漫画《区块链技术上的呆伯特》：

管理者：我认为我们需要建造一个区块链。

呆伯特：糟了。他真懂自己说的东西吗？还是在一个交易杂志的广告里看到的？

呆伯特：你希望你的区块链是什么颜色的？

管理者：我认为淡紫色的内存最多。

在上述例子中，斯科特·亚当斯描绘了层级化结构出现问题的其中一个标志——管理者在获得一定权力后却无法了解实现有效的领导技能所需的知识。

与具有进步管理思维（如何实现高效、创新的组织）相结合后，第一代的互联网让具有此类思维的管理者们改变了工作布署及业绩、赞誉和晋升机制运用的从上至下的架构。

不管怎样，中心化的层级体制是一种惯例。从互联网的早期开始，人们就注意到其去中心化、网络化和赋权的特性。小组和项目开始成为内部组织架构的基础。电子邮件让人们可以在机构内的组织孤岛之间进行相互协作。社交媒体降低了内部协作的成本和交易成本，公司能够更容易地与供应商、顾客和合作伙伴连接起来，这也使得公司的边界不再那么封闭了。

不过，现今的商业化社交媒体工具正在帮助很多公司实现一个新层次的内部协作体系。作为真正权力去中心化的标志，赋权在商业领域中非常重要；而一些公司已经在试验或实施从矩阵管理到全体共治这类新概念，其成效各有不同。

实际上，现在很多人已经达成共识，认为责任、职权和权力的分散通常会带来积极的结果：实现更好的商业功能，顾客服务及创新。不过，这样的机制在实践中谈何容易。

互联网也没有降低经济学家们所谓的“机构成本”，即为确保公司内每一个人都是根据雇主利益行事所耗费的成本。实际上，诺贝尔经济学奖得主（是的，这个故事里出现了不少诺贝尔经济学奖得主）约瑟夫·斯蒂格利茨认为这些公司的庞大体积及明显的复杂程度提高了机构成本，即使在公司的内部交易成本已经大幅下降的情况下。因此，这也导致了首席执行官与一线员工之间存在巨大的薪酬差距。

那么，区块链技术在这个问题上能发挥什么样的作用呢？它能够如何改变公司内部管理和协调的方式？通过智能合约和空前的透明度，区块链不仅能够减少公司内部和外部的交易成本，也能极大显著地降低机构在各个层级的管理成本。这些改变又会让人们更难通过投机取巧去欺骗系统。这样，公司不仅能降低交易成本，还能解决最明显的问题即机构成本。尤查·本科勒告诉我们，“区块链让我最为兴奋的地方是它让人们能够以一个组织所具备的持续和稳定特性互相协作，但不会有组织里面那种层级机制”。[27](#)

这也意味着管理者应该准备迎接在协调资源和行事过程中所需要的极大透明度，因为股东这时将能够观察到这个过程中的低效问题、不必要的复杂性、高管的薪酬与其实际贡献价值之间的巨大差距。记住，管理者并不是公司所有者的代理人；他们在公司里扮演的是中介角色。

4. 建立信任所需的代价——我们为何要互相信任？

就如我们已经解释过的那样，商业和社会中的信任是对另一方将会做到诚实、考虑对方利益、承担责任和透明性的一种期望——即预期他们会以正直的原则行事。²⁸建立信任需要解决很多问题，而很多经济学家和其他学者认为垂直化管理的公司存在的原因是因为在公司内部建立信任要比在公开市场上容易得多。在这个诚信状态不容乐观的时代，公司所面临的挑战不仅是解决“能信任谁”的问题，还有如何能让外部的资源对公司产生信任。

确实，经济学家迈克尔·詹森及其同事们认为正直性是一个生产要素，这并不是他们的首创，不过他们的论述是最有说服力的。他们认为在金融世界里看似永无尽头的骗局及其对价值和人类福祉所带来的严重影响表明了往金融体系中引入更多的正直性是非常重要的。对他们来说，这并不是一个道德问题，而是一个在金融经济体系里“显著提高经济效率、生产力及聚集人类福祉”的机会。对他们来说，“正直性对个人或组织来说有着重要的经济意义（对价值、生产力、生活质量等因素而言）。确实，作为一种生产要素，正直性与劳动力、资本和技术有着同样的重要性”。²⁹

一系列违反正直性的举动让华尔街失去了人们对它的信任（甚至差点就把资本主义终结了）。不过它们已经改变了吗？它们以后会改变吗？在过去，公司的社会责任的推崇者认为公司“可以通过做好事走向成功。”我们还没看到过相关的证据。很多公司通过作恶的行为赚取了不少的利润，如通过在发展中国家剥削员工、将污染这类的成本转移到社会上以及凭借垄断地位盘剥顾客。2008年的金融危机确实让我们看到了一些公司“因作恶付出了很大的代价”。大型的银行经历了重大的损失后才意识到了这一点，在2008年之前它们之中有不少银行每年赚取20%以上的净资产收益率，而今年有不少银行的净资产收益率已经显著低于5%了，甚至有一些银行连资金成本也没法赚回来，从一个股东的角度来看，这种银行不应该再存在了。³⁰

若从现实考虑，华尔街有可能听从迈克尔·詹森的劝告并以正直的要求行事吗？当然了，赚取私利和短期收益的倾向在西方金融体系中已经是根深蒂固了。

现在来考虑一下区块链技术和数字货币。如果各个参与方无须互相信任，也可以根据诚实、承担责任、考虑对方利益和透明性的原则行事——因为这些是金融体系技术性平台的根基，这样会带来什么样的改变？

史蒂夫·奥莫亨德罗给我们提出了一个很有说服力的例子。“若有一个来自尼日利亚的人希望购买我在售卖的一个东西，我将会保持高度的警惕性，我不会接受一笔来自尼日利亚的信用卡或支票付款。现在，通过这个新的平台，我知道我可以信任这个平台，而且不需要引入因建立信任关系所需的成本。因此，它能让以前不太可能的交易方式具有可行性”。[31](#)

这样，华尔街的银行家们并不需要将正直性植入到他们的DNA和行为之中；区块链的发明者已经将正直性植入了软件协议里，并将它部署到整个网络中，这为金融服务产业带来了一个新的公共设施。这个好消息意味着金融服务产业能够重新构建并持续维护信任。

区块链技术能极大地降低搜索、合约、协调和建立信任的成本，对公司来说，这不仅能够更容易地对外开放，也能与外部的参与方建立信任关系。在这种机制下，为自己谋取利益也意味着实现每一个人的利益。欺骗这个系统的成本远远高于依据该系统设计原则去行事的成本。

这并不是说公司品牌甚至行事伦理是不重要的或不再被需要了。区块链帮助确保正直性，因此信任是在双方之间的交易中存在的。它也帮助实现透明性，这是一个信任的关键要素。不过，就如作家和技术理论家戴维·蒂科尔所说，“信任和品牌不仅是确保完成一项交易。它们还是与质量、乐趣、设备或服务的安全性、威望及从容性有关的。在今天全

球气候变暖的大环境下，营造最佳品牌的方式是透明性，以及产出对环境、社会及经济负责的可证实的重要结果”。[32](#)

通过智能合约，高管们就需要对其行为负责了。通过软件的执行和结算，他们必需履行他们的承诺。公司能够以高度的透明性将各种关系进行编程（安排），这样每一个人都能够了解到各方的角色和责任。总的来说，不管他们是否愿意，也必需以一个考虑其他参与方利益的方式行事，因为这个平台要求这样做。

决定公司边界

总的来说，让公司与其供应商、顾问、顾客、外部的同业社区及其他机构分离开来的边界将会越来越难定义了。或许同样重要的是，它们将会不断地改变。

即使有了区块链，公司还是会继续存在的，因为在公司内部进行搜索、合约管理、协调和建立信任的机制相比于公开市场来说性价比是更高的（至少对很多事情而言）。有一种想法被称为“自由职业国”，即人们可以在公司的边界之外工作，这种想法是一种错觉。创建了区块链研究学院的梅拉妮·斯旺说道，“公司需要什么样的规模才能实现最佳的业务效率？这并没有一个标准答案，人们有时作为个人或在线自由职业者参与工作。”对她而言，将会有新型的“由围绕项目达成合作关系的个人或组织所构成的灵活性极强的商业实体”。她将这种新式的公司形式看成是行会，行会是在工业化以前的时代，由在某个特定的城镇一起工作的商户或店主组成的联合体。“我们还是需要有组织承担协调机制。不过这种新型的团队协作模式的具体架构现在还不是很清晰。”[33](#)

今天，我们时常听到“公司应该关注他们的核心”的看法。不过，当考虑到区块链技术将会带来交易成本的下降时，什么是公司的核心？在

公司的核心总是不停变化的情况下你如何对其进行定义？

看来，每一个人对与公司生产力和竞争力最大化相匹配的规模有着不同的定义。我们考察的很多公司对此并没有清晰的想法，似乎是选择了鲍勃·迪伦（Bob Dylan）的方法去决定什么是内部的、什么应该是外部的（“你并不需要一个气象员也能知道风向”）。例如，后勤部门处理流程经常被描述成一种“容易的事”，但其依据并不明显。

有一些观点是更严密的。根据加里·哈梅尔和C.K.普拉哈拉德提出的核心能力的观点，公司通过掌握某种能力实现竞争优势。公司所掌握的核心能力对其至关重要，而其他的一些能力可以从外部获取。³⁴不过，公司或许会掌握一些与其关键任务无关的活动。这些能力还应该保持在公司内吗？

战略专家迈克尔·波特对此有一种隐含的看法，即竞争优势来源于活动，特别是来源于互相强化的活动所组成的网络（作为一个整体，这些活动难以被复制）。这其中重要的并非业务的某个环节，而是它们是如何互相联系并在一个独特的活动系统中互相强化。竞争优势来源于由各种活动所组成的系统的整体；系统内的任何个体活动可以被别人模仿，但竞争者们无法实现同样的好处，除非他们有能力复制整个系统。³⁵

其他人认为公司总是应该保留与关键任务相关的功能和能力——为了生存和走向成功，公司必需认清这一点。但对电脑公司来说，制造电脑是关键；不过戴尔、惠普和IBM将这些活动的大部分外包给Celestica、Flextronics或Jabil这样的电子产品制造服务公司。对一个汽车生产商来说，车辆的最终组装是关键任务，但宝马和梅赛德斯将这些活动外包给了麦格纳（世界第三大汽车零部件供应商）。

斯坦福商学院教授苏珊·阿西的论点颇有说服力：“可能会有一些关键任务的功能，如大数据的收集和分析工作，这些事情若搬到公司外进

行的话风险是比较高的，即使你在这个领域并没有独特的能力”。³⁶确实，可能会有一些如数据分析这样的事情，其生命力取决于独特的能力，这对在外面寻找合作伙伴可能会带来一些相关的风险。不过，其实可以在战略上利用外部资源去建立内部的能力。

我们的观点是公司边界定义的起点是了解你的产业、竞争者和有获利型成长空间的机会——并用这些知识作为建立一个商业战略的基础。然后，区块链开创了建立网络和联系的新机会，每一个管理者和知识工作者需要随时考虑这点。公司边界的选择并不是简单地由高管们决定，那些希望为创新和高绩效而掌握最佳能力的人都可以参与进来。有一个重要的问题我们是需要提一下的，就是你不能将你的公司文化外包出去。

分析模型

若考虑到区块链技术能如何用于公司外部资源的利用上，公司现在对那些与竞争力至关重要的商业活动或功能可以做出定义了——它们是关键任务，同时也具备足够独特的特性，以确保差异化价值的实现。

（参考图4.1.）

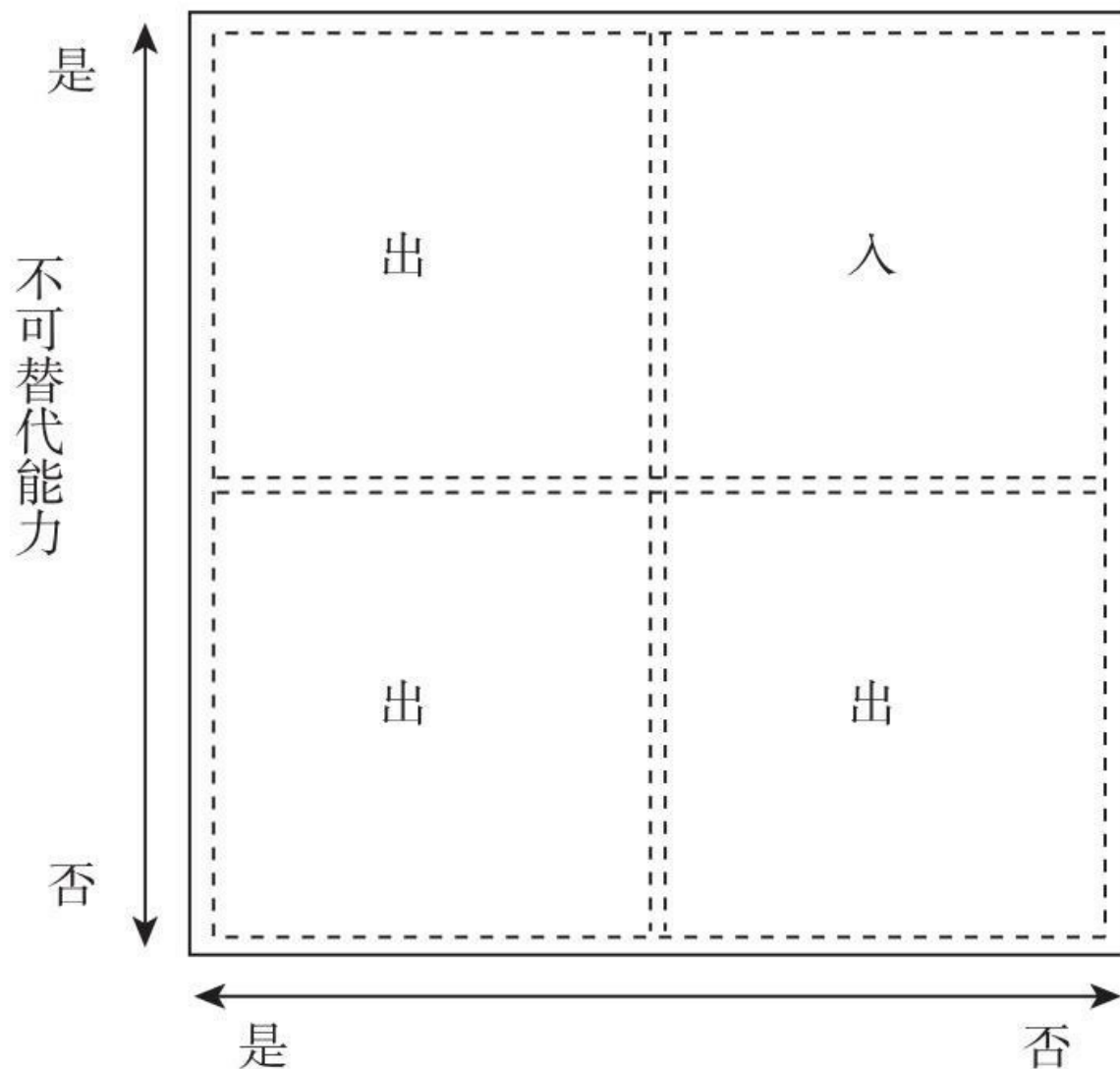


图1 业务核心能力

不过，这个“入-出”的模型只是在任何特定阶段对公司边界进行定义的起点。在定义“什么是最基本的”这个问题上，公司需要考虑其他什么因素？至于将活动外包还是在公司内实现的问题上，有什么因素会影响这个选择？

破解你的未来：边界的决定

当考虑公司边界如何定义的问题时，公司应该开始用区块链对以下

事项进行全方位观察并达成共识——在它们的业务中，什么是唯一的，什么是关键任务？我们来重新讨论约瑟夫·卢宾和ConsenSys的案例，毕竟它们预示了基于区块链的企业的运作手法。记住，ConsenSys仍处于早期阶段，它的业务可能会受到很多不利因素的影响。我们仍然还是可以从这个公司的例子中进行学习。

1.有什么合作伙伴可以更好地完成某项工作？具体来说，我们如何利用新的“群众生产”社区、创意集市（ideagoras）、开放平台及其他区块链商业模式来获益？ConsenSys这个公司能够将一些杰出的专家组织起来完成工作，即使很多专家是在公司的边界之外的。

2.在区块链技术下，公司边界的经济学问题是什么——合作的交易成本与在公司内部保留、开发某项业务的成本哪个更高？你能开发一个核心元素是模块化的、可重用的智能合约套件吗？ConsenSys使用智能合约以降低协调成本。

3.技术上的互相依赖性与模块化相对比，程度如何？如果你对那些能够实现模块化的商业部分进行定义，那么你就可以很轻易地在公司外部重新配置这些部分。ConsenSys对软件开发制定了标准，并提供对多种软件模块的访问权，这样它的合作伙伴们能够在上面搭建应用。

4.你的公司在管理外包工作这方面的能力如何？智能合约能增强那些能力并降低成本吗？从一开始，ConsenSys就是一个区块链公司，其首席执行官约瑟夫·卢宾拥抱该科技和一种经过改进的全体共治制度，我们也能看到那七个设计原则在发挥作用。

5.有人认为这其中存在机会主义的风险，即一个合作伙伴可能会蚕食你的基本业务，就如有观点认为富士康可能会蚕食智能手机厂商的业务一样，这其中的风险有多高？ConsenSys希望通过由人才分享其创造成果的激励机制去建立忠诚度，从而应对这个挑战。

6.在组织的进一步网络化（和收缩）的过程中，会存在法律、监管或政治上的障碍吗？对ConsenSys来说，目前还没有碰到过相关的问题。

7.创新的速度和节奏对公司边界划分的决定来说是非常重要的。有时公司不得不为一个战略性的功能寻找合作伙伴，原因是他们无法在最短时间内自己开发出来。合作关系协议可以成为一个占位符。建立合作关系会帮助我们建立一个能提高竞争优势的生态系统吗？这就是ConsenSys的策略：在以太坊平台上建造一个由协作者组成的网络，培育这个平台和生态系统，最终提高所有环节的成功概率。

8.会有失去对某些基本要素（如一个产品或网络架构）的控制的风险吗？公司必需明晰价值链的哪个部分将会是创造和捕捉价值的关键。如果这些部分转让出去了，公司就会走向失败。以太坊平台为ConsenSys提供了一个基础架构。

9.有什么能力（如数据资产的利用）是必需成为你的企业及其所有运作流程的基础框架的一部分？即使你缺乏某个特定的能力，你也应该将与他人合作视为一个过渡性的策略，最终目标还是为了在企业内部发展出这方面的专才和能力。区块链技术将会带来一系列新的潜能，这些潜能都需要铭记在每一个员工的心中。你不能将公司的文化外包出去。

第五章

新商业模式:在区块链上寻找新机会

Airbnb是在2008年金融市场崩溃前的一个月成立的，现在已经成为一个价值250亿美元的平台。它以市值和房源计算都是世界上最大的房源供应商。不过，房子的实际拥有者们只收到了他们所创造价值的一部分。国际汇款需要通过西联汇款进行，每笔交易需要收取10美元的手续费及额外的外汇转换费用，其结算时间也非常长。Airbnb存储数据并利用它实现经济利益，而房东和顾客都担心隐私保护的问题。

我们与区块链专家迪诺·马克·安格里蒂斯进行了头脑风暴，旨在设计一个区块链上的Airbnb竞争者。我们决定将这个新的商业模式称为“BAirbnb”。它更像是一个由成员所拥有的合作社。所有的收入（除了经常性费用）会流到它的成员手中，这些成员可以控制平台并进行决策。

BAirbnb VS.Airbnb

BAirbnb是一个分布式应用程序（Dapp），它是由一个在（用于登记房源列表的）区块链上存储数据的一组智能合约所组成。BAirbnb有一个简洁的界面：用户可以将他们的房产信息和照片上传上去。¹为了提高每一个人的商业决策质量，这个平台为供应商和承租人保留声誉评分。

若你想租一个房子，BAirbnb软件会在区块链上扫描和过滤所有满足你条件的房源（如离埃菲尔铁塔10英里内，有两个卧室，只接受4星级以上的评分）。你的用户体验跟在使用Airbnb的时候会差不多的，

除了这时你是通过加密过的并用密码学签名的信息在一个点对点的网络上进行沟通，而不是将这些信息存储在Airbnb的数据库里。²只有你和房源的所有者能够阅读这些信息。你们可以互相交换电话号码，而这在Airbnb上是不允许的,因为它不想放弃未来的中介服务收入。在BAirbnb上你和房主可以在区块链之外进行沟通和交易，不过你还是应该在区块链上完成交易的，这有几个方面的原因。

声誉度

由于网络在区块链上记录交易，每一个用户的积极评价都会提高你相应的声誉度。可能得到负面评价的风险会让每一方都保持诚信。记住，那些声誉度较高的人可以在多个去中心化应用程序上使用同样的身份，并持续从其优良的记录中获益。

身份验证

由于我们并不与一个代表我们去检查身份ID的中心化系统打交道，双方都需要确认对方的身份。区块链从一个称为“VerifyID”的身份验证应用程序中调用一个合约，这是BAirbnb、Suber（区块链上的Uber）和其他去中心化应用程序用于检查现实世界身份的（智能）合约之一。

隐私保护

“VerifyID”并不追踪交易或将所有交易存储到一个数据库里。它在收到一个校验公钥（身份）的申请时，只会简单地返回一个真或假的结果。不同类型的去中心化应用程序可以调用“VerifyID”，不过“VerifyID”永远不会知道交易的细节信息。这种将身份与具体活动隔离的做法极大地增加了对隐私的保护。

降低风险

房屋所有者当前将顾客的身份和财务数据存储在自己的服务器上，而这些服务器是可以被入侵和泄露资料的，这样会给房屋所有者带来法律风险和很大的责任。在区块链上，你不需要将你的信息托付给一个供应商；这里面根本就没有一个中心化的数据库可以被入侵和导致资料的泄露。这里面只有点对点的独立的“假名”交易。

保险

现时，Airbnb为房屋所有者提供100万美元的保险，以应对盗窃或损坏的风险。在BAirbnb上，房屋所有者可以使用BAirbnb保险Dapp，像你这样有着良好声誉度的租户会有更低的保险费率，从而避免了补贴那些不够谨慎、粗心大意或不爱护财物的租户。当你提交了一个租房的申请，BAirbnb将你的公钥（身份）发送到保险合约里面并等待回答。保险Dapp会联系一系列可信的供应者，而假冒的保险公司将会被排除。保险公司会通过自主运行的机构软件对合约所输入的信息实时进行计算——如房屋所有人的房产市值、他们需要多少保险额度、房屋所有人的声誉度、你作为租户的声誉度，以及租金价格。BAirbnb会接受最优惠的保险费率并将其加到房屋所有者希望收取的日租金里。区块链在后台处理这些计算任务，房屋所有人和租户有着与Airbnb差不多的用户体验，不过得到了一个更优秀、更公平的价值交换体验。

支付结算

当然了，在区块链上你可以在几秒时间内将款项发送给房产所有者，而这在Airbnb上需要几天的时间。所有者通过智能合约可以更容易地管理押金，一些人会使用托管交易账号以逐步支付款项（每晚、每星期、每小时等），或在彼此的同意下将款项全部支付完毕。若出现了涉及智能合约的纠纷，各方可以申请仲裁。

使用智能锁接入房产（物联网设备）

一个连接到区块链上的智能锁知道你什么时候已经付款了。当你到场后，你的带有近场通信（NFC）技术的智能手机可以用你的公钥签发一条信息，作为付款成功的证据，而智能锁就能被打开。所有者无须留下钥匙，也无须亲临该房产，除非他们想来打个招呼或解决某些紧急情况。

你和房屋所有者现在大约已经节省了15%的（在Airbnb上会收取的）费用。结算是可以保证的、即时完成的。在签订国际合约的时候，也没有外汇转换的费用。你无须担心身份被盗。一些地方的政府无法强迫BAirbnb给出所有的历史出租数据。这是真正的价值共享机制，而顾客和服务提供商都是赢家。

全球计算：分布式应用的兴起

在我们考察其他如BAirbnb这样的潜在的分布式商业实体之前，先讨论一下这项底层技术是如何推动中心化的。在区块链出现之前，中心化的组织一直在控制计算能力。

在企业级计算的前十年，所有的软件应用是在用户的电脑上运行的。通用汽车公司、花旗银行、美国钢铁公司、联合利华及美国联邦政府拥有大型的数据中心，用于运行各种专有的软件。公司从供应商手上（如80年代的巨头CompuServe）进行算力的租用或“时间分享”，以运行它们自己的应用程序。

随着个人电脑的发展，软件市场变得专业化了：一些公司开发客户端应用，另一些公司开发服务器应用程序（一台充当主机的电脑）。通过互联网的广泛使用（特别是万维网），个人和公司都能用他们的电脑去分享信息——最初是文本文档，后来是图像、视频或其他多媒体内容，最终是软件应用程序。³分享使得信息领域变得更民主化了，但这

个阶段只延续了很短的时间。

在1990年，一种新型的“时间分享”的模式出现了，最初是叫“虚拟专用网络”，然后是云计算。云计算让用户和公司在第三方的数据中心里存储和处理它们的软件和数据。像Salesforce.com这样的新创技术公司通过使用云模式给顾客省下了开发和运行自己的软件所需的成本，从而实现了不少的收入。像亚马逊和IBM这样的云服务提供商创造了规模极大、市值高达数十亿美元的业务。在2000年左右，像Facebook和Google这样的社交媒体公司创造了运行在它们自己的大型数据中心的服务。这个中心化的趋势一直在持续，像苹果这样的公司将网络的民主化架构转换成如苹果商店（Apple Store）这样的专有软件平台，顾客在里面获取专有的软件，这并不是开放的网页，而是严密把关的地方。

在数字纪元，大型的公司一次又一次进行了合并，在它们自己的大型系统中创建、处理、拥有或收购各种应用程序。中心化的公司使得中心化的计算架构最终带来中心化的技术和经济权力。

这是一些危险信号：单一的控制权让这些公司很容易面临灾难性的崩溃、欺诈和安全问题。如果你曾经是Target、eBay、摩根大通、家得宝或Anthem，甚至是Ashley Madison（为已婚人士提供约会服务的网站），美国人事管理办公室（第二次被入侵了！）或Uber的顾客，你就能感受到2015年这些系统被入侵所带来的痛苦。⁴公司不同部分的系统在互相沟通的时候依然面临着重大的挑战，更不用说与外界公司系统沟通的时候了。对我们用户来说，这意味着我们永远没有控制权。其他公司用他们的隐含动机和目标为我们定义相关的服务，而这可能与我们的目标相冲突。就在我们产生宝贵的数据时，其他人控制这些数据并用其谋取巨大的财富（或许是史上规模最大的），而我们中的大部分人只得到很少的好处或补偿。这其中最可怕的是中心化的力量使用我们的数据去创造我们每一个人的形象档案，并可能会利用这些档案向我们兜售东西或监视我们。

现在区块链技术已经出现了。任何人可以在这个平台上传一个程序，让其自动执行，并且有密码学经济机制⁵在背后起作用，这样确保了程序会以当初设计的目标安全地执行。这个平台是开放的，而不是在一个机构之内，它含有不断增加的资源，如用于鼓励和奖励特定行为的数字货币。

我们在进入数字化革命的一个新纪元，人们可以进行分布式软件的编程和分享。就如区块链协议本身是分布式的那样，一个分布式的应用程序或Dapp（去中心化应用程序）会在很多计算机上运行，而不是在一个单一的服务器上运行。这是因为区块链上运行的所有计算资源可以在整体上视为是一台计算机。区块链开发者加文·伍德认为以太坊是一个处理平台并给出了一个解释：“世界上只有一台（统一协作的）以太坊计算机”，他说道，“它也是多用户的——任何曾经用过它的人都会自动登录进去”。因为以太坊是分布式的，并以最高标准的密码学安全机制构建，“所有的代码、处理流程和存储机制是在应用程序自己的密闭空间里存在的，没有人能够操纵这些数据”。他提到这台“世界计算机”里整合了这些关键的规则，可谓是“虚拟的硅晶片”。⁶

至于去中心化应用程序（DApps）的领域，在区块链出现之前已经有一些预热的例子了。点对点的文件分享应用程序BitTorrent展示了Dapps的力量（当前它占据了互联网上所有流量的5%）⁷。音乐爱好者、公司和其他媒体免费分享它们的文件，由于它们没有中心化的服务器，权力机构也无法将其关闭。敢于打破常规的程序员布拉姆·科恩发明了BitTorrent，但他对比特币并没有这么热情，原因是围绕比特币进行的商业活动太多了，他认为“这场革命并不应该货币化”。⁸

我们中的大多数人认为通过技术创新创造收入和经济价值是积极的，只要这场数字化革命没有被少数人货币化。有了区块链技术，去中心化应用程序几乎有了无限的可能性，因为它将Dapps带到了一个新的层次。Dapps和区块链可能会像歌曲描述的那样，“爱和婚姻，爱和婚

姻，就如马和马车般结合在一起”，联合发挥作用。Storj这个公司建造了一个分布式的云存储平台及一系列的Dapps，让用户可以安全地、廉价地、秘密地存储数据。这里面没有一个中心化的机构可以访问用户加密过的密码。这个服务消除了中心化数据设施的高成本；它是非常快的；它还对用户出租闲置磁盘空间的行为给予报酬。这就像电脑空闲存储空间领域的“Airbnb”。

Dapp的王者：分布式商业实体

Dapps如何能将更高的效率、创新和响应能力融合到公司架构里？我们能利用Dapps实现什么新型的商业模式并创造价值？如果大型机构今天正在利用互联网所带来的好处，我们如何从“外包”和“商业网”的层面更进一步，实现真正去中心化的创新和价值创造模式，最终使得繁荣及数据的所有权和财富得以广泛分布？我们描绘了自己所认为的4个最重要的创新成果，并将其放置到两个矩阵里。

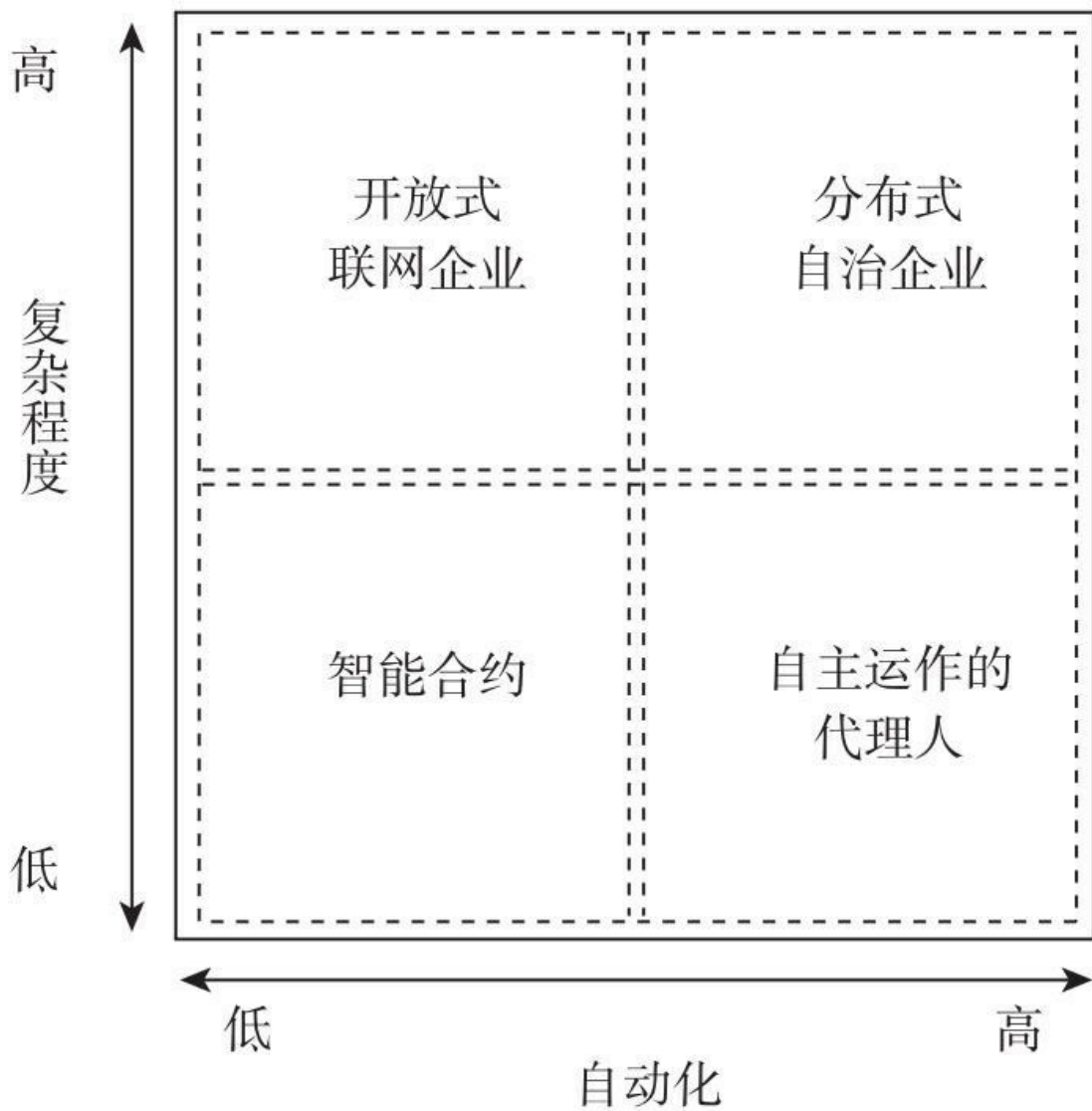


图2 分布式商业模式

Y轴表明了在这个模型中人们的参与度。在最左边的位置，这个模型需要一些人们的参与。在最右边，这个模型不需要人们的参与。

X轴描述了这个模型功能的复杂程度，而不是技术上的复杂程度。在最下面的位置标明这是可以执行简单功能的模型。在顶部的位置标明这是可以执行不同功能的模型。

这些是区块链经济体系的所有部件，因为它们使用区块链技术和加

加密货币（通常会有）作为它们的基础。智能合约是最基本的形式：它们涉及了一些需要人们参与的复杂性，特别是在多重签名协议的形式中对人们参与的需求更多。随着智能合约复杂性的增加及与其他合约进行活动，它们可以成为我们称为“开放式联网企业”的一部分。如果我们将“开放式联网企业”与自主运作的代理人——无须人们参与也能自动制定、执行决策的软件组合在一起，我们就得到了被称为“分布式自治企业”的形态，它只需少量甚至无须传统的管理体制或层级化体制也能为客户创造价值并为所有者创造财富。我们认为数千或上百万人可能会通过协作创造事业，并分享其创造的财富，而这是财富的分发而不是重新分配。

开放式联网企业

智能合约让公司能够与以前可能不会有业务来往的新类型供应商和合作伙伴去构建智能的、自我执行的协议，其中的费用非常低廉。智能合约若集合在一起，就可以让公司更像网络，让公司的边界更有渗透性和流动性。

区块链技术同时也降低了罗纳德·科斯所提到的搜索成本和协调成本，这样公司可以分解成更多的高效网络。一个汽车公司可以通过在线扫描统计服务数据去检查其供应商的可信性。很快，该公司就可以在区块链上的一些产业市场上输入“轮轴”或“窗户玻璃”并在线商讨价格。

我们可以将这个简单的场景扩展为寻找一个替换件、供应链合作伙伴、协作者或用于管理分布式资源的软件的场景。你希望从中国采购钢铁，从马来西亚采购橡胶，或从堪萨斯州的威奇托采购玻璃？没问题。以Dapps的形式进行运作、为每一种商品而设的去中心化在线清算场所让采购商可以达成关于价格、质量、交货日期的合约，这个过程只需要用鼠标点击几下就能完成。你将会有一个详尽的、可搜索的记录，其中包含了以前的交易信息——不仅是不同的公司过去的评分状况如何，还

有精确到它们是如何履行承诺的。你可以在虚拟的地图上追踪每一个批次货物的运输状况，展示出其精确的位置。你可以对商品的运输计划进行仔细地管理，确保它们及时到达，那么就不需要仓库了。

自主运作的代理人

想象一下，若有一个软件可以用自己的钱包和学习、适应的能力在互联网上工作，执行其创造者所定下来的目标，购买其生存所必需的资源（如运算能力），同时还能给别的组织提供服务.....

自主运作的代理人（autonomous agent）这个术语有很多种定义。⁹ 在本文中，它代表能够根据某个创造者的命令行事，并从其环境中提取出信息及有能力独立地做出决定的一种设备或软件系统。我们可以将某些自主运作的代理人称为有“智能”的，即使它并没有全面的智能。不过，它们并不是“只是一种计算机软件而已”，因为它们能够改变实现其目标的方法。随着时间的推移，它们可以感知并对它们的环境做出回应。¹⁰

“计算机病毒”是被引用得最多的自主运作代理人的例子之一。计算机病毒通过在机器之间复制自身实现其生存，这个过程并不需要人为干预。在区块链上放置一个病毒显然是更困难的，成本也更高，因为这可能必需付费给另一方与之互动，网络可以很快地识别出它的公钥，极大地降低其声誉度，或者不再确认它的交易。

以下是一些具有积极意义的区块链的例子。一个云计算服务可以从不同的来源租用计算机运算能力，通过与其他有闲置资源的计算机达成租赁协议，有可能成长成像亚玛逊那样一样大的规模。¹¹ 一个由社区、公司、个人或其自身所拥有的无人驾驶汽车在城市里面四处载客，并收取相应的费用。我们对以下的代理人十分感兴趣：它们应该可以进行交

易、获取资源、进行支付或为其创造者带来价值。

创建了以太坊区块链的维塔利克·布特因为这些代理人建立了一套理论，并提出了一套分类法以描述它们的进化。在其中的一端，有单一功能的代理人，如病毒，其运作过程是为了实现它们有限的目标。然后就是更聪明、功能更多的代理人，如一个从供应商（如Amazon.com）上租用服务器的服务。一个更高级的代理人可能会找出从任何一个供应商里租用服务器的方法，然后使用任何搜索引擎去查找新的网站。一个更有能力的代理人甚至还能升级自己的软件，并适应新型的服务器租赁方式，如对终端用户给予报酬以租用他们未使用的电脑或磁盘空间。下一步就是能够发现和进入新的产业，从而通往物种进化的新台阶，即实现完全的人工智能。[12](#)

气象网络

一个自主运行的代理人能够使用区块链技术去进行气象预报从而赚取利润吗？我们可以想象一下2020年的场景。到那时候，世界最优秀的气象预报服务是来自一个由智能设备所构成的网络提供的，而这个网络在全世界范围内测量和预测气象。那一年，一个自主运行的代理人BOB被释放到网络上，与其他设备一起协作，创造出一个商业模式。下面是BOB的工作方式。

分布式环境传感器（气象探测节点）会被安装在电线杆、人们的衣服、建筑的屋顶上和到处行驶的车辆里，也可以与卫星相连接，最终形成一个全球的网格网络。这样，就不需要互联网服务提供商来提供网络连接了。它们不会将数据存储在一个中心化的数据库里，而是存储在区块链上。[13](#)这些传感器之中，有不少是用太阳能供电的，所以无须连接到供电网络了。这些传感器能在长时间内高效运作。

在这种模式下，区块链负责几个功能的处理。首先，它解决了支付

问题。每一个气象节点每隔30秒都会收到一笔小微付款，是用于激励其提交的对应世界上某个特定地区的准确气象测量数据（温度、湿度和风等）。

区块链也会储存所有的气象节点的交易。每一个气象节点用其公钥对其所有数据进行签名并存储在区块链上。公钥是一个气象节点的识别标志，能够让其它实体用于其声誉度的评估。当节点产出了准确的气象数据后，它的声誉度就会提升。如果一个节点坏了或者被篡改了，产出了不准确的数据，声誉度就会降低。声誉度较低的节点获取的比特币要比声誉度较高的节点少很多。这个机制的受益人是这个应用程序的创造者——不管是个人、公司或合作社组织。

区块链也让数据提供者和数据消费者可以用点对点的方式参与到一个单一的、开放的系统中，而不是订购全球范围内数十个中心化的气象服务数据，更不需要编写软件用于这几十个服务器的API（应用程序接口）的沟通。通过智能合约，我们可以实现全球性的“气象数据市场Dapp”，数据消费者可以实时地给数据出价，并以一个统一接受的格式接收到该数据。中心化的数据提供商可以抛弃其专有系统和个人销售任务，然后成为全球可访问的气象数据市场Dapp的数据提供商。

全球气象DApp: 传感器的网络

在互联网的第一个时代，技术创新只在中心开展。中心化的实体，如能源公司、有线电视公司、中央银行，是可以决定什么时候升级网络、什么时候支持新功能以及谁有访问权。创新不能在“边缘”开展（如使用网络的个人）因为密闭的系统的规则和协议意味着任何设计成与网络进行互动的新技术必需经过中心化权力所有者的同意才能开始运作。

不过，这种模式是低效率的，因为它们无法实时知道市场的需求是什么。它们必需进行合理的推测，而这些推测的准确性往往不如市场的

实时需求。所以我们就有了WeatherCorp，它是一个中心化的服务，具体内容是安装传感器和发射卫星，这样它就可以将数据卖给少数希望订阅数据的人。

区块链让任何实体成为一个气象预报提供者或气象数据消费者，准入门槛很低。这只需要买一个气象节点（weatherNode），放在你的屋顶上，并与全球气象数据市场DApp节点连接起来，你就可以开始获得收入了。如果你可以对你自己的屋顶气象进行改造让其精度变得更高，那就更好了。你在边缘进行创新，而市场会给予你相应的奖励。在开放网络上，对创新的激励机制能够促进效率的提高，在这一点上比封闭式网络做得更好。

机器人的竞赛

这些系统里面会有利益的冲突吗？如果气象节点开始扩展其能力并进入农作物保险市场，会出现认知上的差距吗？农民放置的气象节点希望强调旱灾所带来的影响，而保险公司的气象节点却称旱灾影响非常小。代理人（节点）的所有者和设计者需要运作的透明度。如果双方尝试通过偏见的立场进行传感器数据的过滤，那么他们各自的声誉度都会下降。

维塔利克·布特因指出创建自主运行的代理人是一项很有挑战性的工作，因为这些代理人的生存和成功都依赖于在一个复杂的、变化极快的甚至是敌意的环境里保持运行。“如果一个网页服务商希望作恶，它们或许会定位到某些服务的服务器，然后将它们替换成可以作弊的节点；一个自主运行的代理人必需能够检测到这样的作弊行为，并从系统中消除或屏蔽这些作弊节点所带来影响”。¹⁴

需要注意的是，自主运行代理人同时也将人格与资产的所有权与控制权分离开来。在区块链技术出现之前，土地、知识产权和金钱等所有

的资产都需要有一个人或由人组成的合法组织持有。安德烈亚斯·安东诺普洛斯认为加密货币完全忽略了人格在其中的作用。“一个钱包可以被一个无人拥有的软件控制，所以有可能存在一种自主运行并控制自己资产的软件代理人”。[15](#)

一个自主运作的代理人可以支付自己的网页服务器，使用进化的算法去传播自身的副本（通过做出细微的改变并让这些副本生存下去）。每一个副本可以包含由它自己发现的或在互联网上进行任务的众包而得到的新内容。随着这些副本中的一部分运作得越来越成功，代理人可以向用户销售广告，所得的收入可以直接进入银行账号或者在区块链上某个安全的地方存储起来，这样代理人可以使用这些不断增长的收入去进行更多广告内容的众包业务并实现自身的传播。代理人会继续重复这个流程，这样能够吸引人的内容会得到广泛传播，并能自己维持运作，而不成功的内容基本上会消亡——因为它没有收入去维持自己的运作了。

分布式自主运作企业

现在，我们建议你坐在《星际迷航》船长的座位上绑好你的安全带。想象一下由有一个名为BOB 9000的东西——在一个复杂的、基于区块链的生态系统中的一系列自主运作的代理人，能够根据任务使命和规则进行相互的协作。结合在一起后，它们会创造出一系列可以出售给人类或各种组织的服务。人类会让这些代理人“充满生命力”，赋予它们完成运作所需的运算能力和资本。它们可以自己采购所需的服务，雇佣人类或机器人，获取如生产能力、品牌设计与推广和市场营销专长的合作伙伴资源，并实时进化。

这种组织也可以有自己的股东，可以是参与众筹活动的数百万人。这些股东提供一个任务使命，如本组织应该合法地将利润最大化并正直地对待其股东。股东们也可以在需要的时候进行投票以管理此组织。与

传统的组织不同的是，传统的组织是由人类去做决定，而在终极的分布式组织里很多日常的决策制定任务可以被编程成为智能的代码。在理论上，这些组织最起码可以在较少甚至无须传统管理架构的情况下运行，每个流程、每个人都根据智能合约里编码好的特定规则和流程运作。在这种组织里，不会有报酬超出其贡献的首席执行官、管理层或公司里的官僚主义，除非这个组织决定雇佣并建造一个。在里面，不会有办公室政治，没有繁文缛节，也不会出现彼特原理所描述的情境中呆伯特型企业，因为技术提供者、开源社区或企业的创始人会为软件设定一个目标，让其自动执行特定的功能。

任何人类雇员或有合作关系的机构会在智能合约的框架下运作。当他们完成指定的工作，就能即时得到报酬——或许不是两星期一次而是每天、每小时或者是每微秒都可以在付款。这个组织并不一定要有拟人化的主体，雇员甚至可能不会知道是一个算法在管理他们。不过他们会知道“良好行为”的规则和标准。考虑到智能合约会将管理科学理论的集合编码进系统中，他们的任务和绩效指标将会是透明化的，大家都会因此而热爱工作。

顾客们可以提出反馈意见，而企业将会平心静气地接受并即时实施改进方案。股东们将会（甚至是频繁地）接收到分红，因为实时会计技术会取代年终报告。这个组织背后的开源软件的创始人制定了一系列的规则，搭建了透明的指导方案和不可侵蚀的商业规则，这个组织将会根据这些透明的规则执行所有的运作流程。

欢迎来到由区块链技术和加密货币所驱动的分布式自主运作企业（DAE），在未来自主运作的代理人可以自我聚合起来，形成一种全新的企业模式。

若你要说这一切听上去是不现实的、无意义的甚至是从科幻小说中提取出来的，那就先考虑一下如下的事情。通过代币（tokens）的使用，像ConsenSys这样的公司已经在内部发行股份了，在无须监管方参

与的情况下进行了股份的公开发行人。你可以用合法的方式记录私营公司的所有权，并在区块链上将这些股份转让给其他人。你的股份证书将能接收到分红并赋予投票权。你的新型“区块链网络公司（blockcom）”是分布式的，它不能脱离某个具体的辖区而存在，但你的股东可以位于世界的每一个角落。想象一下用类似的机制去以债券的形式发行债务——不管是私有公司的债券还是主权国家债券，这实际上是在创造一个债券市场。同样的逻辑可以应用在商品上——不仅是商品自身，还能是该商品所对应的票据，就如芝加哥商品交易所或全球黄金市场的运作一样。

不要以你现在所知道的证券的概念去想问题。想象一下若能有一个全球的IPO，可以有1亿的股东，每人贡献几分钱。这并不完全是天方夜谈——管理和治理机制可以在几百万人拥有可投票归属权的情况下进行大范围的运作。最后，处于金字塔最底层的投资者可以在世界的任何地方参与并拥有一个创造财富的组织股权。在理论上，我们至少能够设计出一个没有高管而只有股东、金钱和软件的公司。股东可以对代码施加相应的影响，这样代码和算法会取代某个层面的代表们（如董事会）。它对繁荣的实现所带来的机会是很显著的，其中的影响丝毫不亚于财富创造机构所有权的民主化。

这是不实际的？或许吧。不过考虑一下，已经有企业在使用以太坊这样的脚本语言去设计这样的功能，最终是为了建立自主运行的模式。另外，还有一些创新者已经在部署可以实现资金多重签名控制的代码。通过众筹活动，很多人在购买公司的股份。DApps已经在为自主运行的代理人引路了。

这个彻底的分布式企业可以有一个钱包，它需要几千个签署人达成共识才能在一项重要的交易上花钱。任何股东可以就这笔钱的收款方提出建议，在与该笔交易有关的事项上管理共识。这样的架构会有一些明显的挑战。例如，需要有一些能够快速达成共识的机制，或者确定谁对该交易的结果负责？如果你在投票中的权重是万分之一，你的法律责任

和负担是会是什么？会有可能出现自我传播的犯罪组织或恐怖组织吗？安德烈亚斯·安东诺普洛斯对此并不担心。他相信网络会管理这样的危险性。“将这项技术带给75亿的人，其中的74.99亿人会用它来做好事，而这样的好事会对社会带来非常积极的影响。”¹⁶

七大开放式联网企业商业模式

若要构建开放的联网式企业，则有可能颠覆或取代传统的中心化模式，甚至进化到早期的分布式自主运作企业，这其中存在着无数的机会。考虑一下这个分布式的模式能如何颠覆或取代金融服务的八项功能，范围包括了零售银行业、股票市场到保险公司和会计师事务所。现有的机构和新的机构都能构建这样的新型商业架构——实现更好的创新、以更低的成本创造更多的价值，并让生产者能够分享到他们所创造的财富。

区块链技术将《维基经济学》里描述的一些新商业模式带到了一个新的层次。¹⁷让我们思考一下，如何通过加入原生的支付系统、声誉系统、无须信任的交易、智能合约及自主运作的代理人（上述是区块链革命的关键创新点）去扩展如下的领域：大众生产、创意集市、专业消费者、开放平台、普通人的新力量、全球工厂和维基（社交）工作空间。

大众生产

大众生产是由无数的志愿者实现的，这样的志愿者们带给你开源软件和维基百科，这些都是能媲美大型的、资金充裕企业的创新性项目。社区成员为了各种原因参与到项目中，这包括了兴趣、爱好、结识其他人或为实现自己的价值。现在，通过引入声誉度系统和其他激励机制，区块链就可以改善他们的效率并用他们所创造的价值给他们支付报酬。

大众生产社区可以是“普通人为基础的大众生产”，这是由哈佛法学院教授尤查·本科勒提出来的一个概念。¹⁸它有时候也被称为“社会生产”，这也是尤查·本科勒提出来的术语——商品和服务是在私营部门的边界之外生产出来的，而且不是由一个公司或个人所拥有。在无数的例子之中，Linux操作系统是最典型的一个（它不被任何人或公司所拥有，但已经是世界上最重要的操作系统了），还有维基百科（由维基媒体基金会所拥有），以及火狐浏览器（由Mozilla基金会所拥有）。大众生产也可以用于指代在私营部门里发生的一种活动，即各方通过群体协作创造出某些东西，但成果并不是为被群体所拥有。

大众生产这种作为一种商业模式，其重要性包含两个方面的原因。首先，大众通过协作，以志愿者的形式生产商品和服务，而公司在这其中会作为管理者并实现商业利益。读者在Reddit讨论平台（流行的外国论坛）上创造内容，不过他们并不拥有这些内容。若按照流量计算，Reddit是在美国规模排在前10名的网站。其次，公司可以利用大量的外部人力资源。IBM拥抱了Linux，并向Linux社区捐赠了价值数亿美元的软件。在这个过程中，IBM省下了本来要用于其专有系统开发的每年9亿美元的费用，并创造了一个承载数十亿美元软件和服务业务的平台。

经验表明若要实现志愿者社区的长期可持续性是一件不容易的事情。实际上，一些最成功的社区找到了补偿成员所做出的贡献的方法。就如史蒂夫·沃兹尼亚克（Steve Wozniak）告诉斯图尔特·布兰德的那样，“信息应该是免费的，但你的时间则不应该是这样”。¹⁹

在Linux的例子中，大多数的参与者收到了来自IBM或Google的经费，以确保Linux满足它们的战略需要。Linux目前依然是社会生产的一个例子。尤查·本科勒告诉我们，“一些开发者被第三方付款来参与到这个项目里这个事实并没有改变Linux的治理模式，也没有改变Linux是由社区共同开发的这个事实”。他认为这已经比那些在公司之间进行协作的所谓开放式创新及分享特定知识产权的模式更有成效。他说

道，“Linux为很多贡献者提供了明显的社会激励动力，因此这可以看成是一个混合模式”。[20](#)

还有，有很多这样的社区里充斥着各种不良行为、无能行为、破坏者和造谣者——那些通过散布煽风点火的、失实的或离题的信息去扰乱社区从而挑动矛盾的人。在这些社区中，声誉机制通常是非正式的，而良好行为也没有相应的经济激励。

通过区块链技术，大众能够为社区的高效贡献者开发出更正式的声誉度机制，以阻止不良行为，成员会预付一笔数额较小的钱，并会基于其贡献而有相应的增加或减少。智能合约降低了交易成本并打开了公司的边界，这样由公司所拥有的社区里，大众可以分享他们创造的价值并为他们所做出的贡献得到经济补偿。

考虑一下Reddit的例子。这个社区已经推翻了中心化的控制方式，不过依然受到来自轻率的、粗鲁的成员的影响。Reddit可以从转移到一个更具分布性的模式中受益，这个模式能回报那些重要的贡献者。ConsenSys已经在开发Reddit的区块链替代方案，就是为了实现上述目标。ConsenSys认为通过提供经济上的激励机制可以改善类似Reddit这样平台的沟通质量，而无须依赖中心化的控制和审查。以太坊平台提供激励机制（可能是实时的），鼓励人们生产高质量的内容并以文明的规则行事，同时也能促进群体的共识。

Reddit本来有一个名为Reddit“黄金”的系统——这是一个可以让用户购买并让他们奖励给为他们带来价值的成员。销售代币所得的收入会用于站点的维护。对用户来说，这样的“黄金”并没有固有的价值。那么，如果有一个真实的、可转让的及基于区块链的货币激励机制，Reddit成员能够开始为对站点良性运行的贡献而得到真正的收入。

维基百科作为社会生产的旗舰象征也可以从这样的机制中受益。现在所有编辑文章的人会得到一个非正式的声誉度，即基于他们编辑过多

少文章、效率如何，并且是通过非常主观的方式进行评价。维基百科社区经常就激励机制进行辩论，不过为7万个志愿者做出某种形式的经济补偿一直都是不现实的。

如果维基百科转移到区块链上——可以叫它Blockapedia [区块链维基百科（结合了区块链与维基百科的词组）]，除了有在一个不可篡改的账本上记录带有时间戳的条目这个好处外，还可以实现更正式的声誉度管理机制，从而奖励良好行为并积累贡献。赞助者们可以资助金钱（或所有的编辑者可以捐赠）到一个托管账户里。每一个编辑者都有一个与其账户价值相连的声誉度。如果她试图破坏一篇文章（例如写上某场大灾难从来没发生过），那么她在账户中的存款价值将会降低，而对于那些毁谤或侵犯他人隐私的行为，她将会失去账户里的存款甚至会面临民事或刑事的后果。有关第二次世界大战的真实事件可以通过多种途径确定下来，例如在区块链上查阅不可更改的事实或通过某些算法展示出就某项事实达成的共识。

你的Blockapedia的保证金可以是与你此前在维基百科或类似平台上的声誉度成比例的。如果你是一个新用户，而且没有声誉度记录，那么你就需要交出一笔较大的保证金才能参与。如果你成功在维基百科上编辑了200篇文章，那么你的保证金要求就可能很低了。

这并不一定是关于将维基百科转换成一个雇佣性质的补偿模式。“这只是一个基于你提供的信息的准确性和真实性而提供的对应现实世界的经济奖惩机制的简单例子。”²¹基于区块链的智能钱包的首席执行官迪诺·马克·安格里蒂斯说道。损害Blockapedia的行为会给你的正式声誉度带来损害，而且也会让你损失金钱。

不过维基百科现在运行得不错，不是吗？并非这样。Andrew Lih在《纽约时报》的一篇文章里写道，在2005年几个月的时间里，有超过60个编辑被提升成管理员。管理员是一个有编辑英语版本文章的特权角

色。在2015年，这个网站甚至连每月更新一个版本都变得很困难了。作为一个志愿者构成的全球组织，其内部存在一些不和谐因素。还有，在移动设备上编辑内容是很困难的。“潜在的维基百科编辑会随着移动设备用户数量的增加而不断降低。”Lih表示维基百科的失落将会是很不幸的事情。“维基百科用这么少的成本、这么多的人力生产出了这么多的信息，这在历史上是从未有过的。这个组织里不存在营利机制和所有者，这让其成绩变得更显著。在这个互联网巨头争霸的时代，这个最无私的网站是值得被拯救的。”²²

总的来说，大众生产社区是处于新型的、联网的价值创造模式的中心位置。在大多数产业里，创新越来越依赖于公共和私营的参与者构成的紧密网络、大型的人才库及通常被融合成新的终端产品的知识产权。就如IBM拥抱了Linux一样，公司甚至可以接入到自我组织的价值创建者所构成的网络中，就如开源运动共同创造价值或实现价值的大众生产一样。

知识产权创造者

在第一代的互联网中，很多知识产权的创造者并没有得到适当的补偿。例如音乐家、剧作家、新闻记者、摄影师、艺术家、时装设计师、科学家、建筑师、工程师等角色，这些人为唱片商、出版商、画廊、电影工作室、大学和大型公司都做出了贡献，而这些组织坚持这些创造者必需将他们的知识产权的相关权利转让给大型的（知识产权）权利管理中心，在这个过程中这些创造者在这些知识产权的价值中能获得的补偿越来越少了。

区块链技术为知识产权的创建者提供了一个新的平台，让他们能够得到其中的价值。可以考虑一种艺术品的数字记录系统，包含防伪证明、状态及所有者。一个新的初创公司Ascribe让艺术家能自己上传艺术作品，并加上水印以证明是确定的版本，还能像比特币那样从一个人的

藏品库中转移到另一个人的。这是很强大的模式。这项技术解决了知识产权世界的类似双重支付问题，甚至比现有的数字权利管理系统都更好。艺术家可以选择是否、何时和何处部署这个系统。

文化基因（Meme）艺术家罗恩·V说道，“艺术品是一种货币。艺术品转变成数字货币的机制无疑是未来的潮流。这是一个良性的步伐”。²³如果某些音乐家、摄影师、设计师、插图画家或其他艺术家的作品可以被数字化并加上水印作为确定性的版本，那么他们就可以使用这项技术将他们的知识产权转化成可以交换的资产，或许还能成为某个特定的拥护者提供的定制化限量版本。艺术家们和博物馆可以使用Ascribe的技术去将某些作品借给其他的个人或机构。²⁴Monegraph这个公司在提供一个类似的服务：它在区块链上整合数字化水印和密码学技术，以用于作品的真伪性证明。艺术家们可以简单地将作品上传到互联网上的一个页面上，并将链接发给Monegraph公司。这个公司会发行一对公钥和私钥，除了与公钥相联系的价值是对该艺术品的数字证书，而不是对应比特币。Monegraph同时也会在推特（twitter）上发一条该证书的公开声明，这是值得注意的，因为美国国会图书馆会对公开的推特信息进行存档。²⁵其他人或许会想声称他拥有该链接，但在这之前已经有两条公开的记录能够证明所有权了。²⁶

有一个位于洛杉矶的初创企业Verisart，其顾问是比特币的核心开发者彼得·托德，它有着更远大的追求。对艺术品的真伪和状况进行证明是一门大生意，而目前大部分是在纸质的条件下进行的，而且是被那些能访问私有数据库的精英专家们所控制的。即使对那些实际上知道自己所寻找目标的人来说，要找出谁拥有某个艺术品、这个艺术品存放的位置及其状况是一件很有挑战性的事情。Verisart正将区块链技术与标准的博物馆元数据组合在一起，以创建一个为艺术品和收藏品而设的公共数据库。这个世界账本将会为世界范围内的艺术家、收藏家、管理员、历史学家、艺术品鉴定师及保险公司提供服务²⁷。通过使用比特币

区块链，Verisart可以将数字化起源技术添加到任何实体作品上（而不只是数字化的艺术品），在参加在线拍卖活动或同意售卖艺术品前，用户将能够在移动设备上检查某份艺术品的真伪、状态和所有权的变化历史。“我们相信这项技术可以促进信任的形成和增加流动性，特别是随着每年670亿美元价值的艺术品市场开始转向私下售卖（点对点）和在线交易”，创始人罗伯特·诺顿这样告诉TechCrunch的，“艺术品的世界并没有崩溃，它只是在保证信任和流动性的过程中太需要依赖中间人了。我们相信一个去中心化的世界账本的出现，结合先进的加密机制以隐藏买家和卖家的身份，对艺术品市场来说是具有吸引力的”。²⁸艺术家们将成为所谓的“利用权力实现经济利益的人”，通过技术签署协议并实时得到收入。

你可以将这个模式应用到其他领域。在科学领域，一个研究员可以为某些限定范围的受众专门发表一篇论文，就如中本聪（比特币发明者）所做的那样，从而得到评估意见和可信性，从而发表给更广泛的受众，而不是将所有的权利转让给一个科学期刊。这个论文甚至可以是免费获取的，但其他科学家可以向作者订阅一份更深入的分析或在线讨论。基于智能合约，她可以公开原始的数据或其他科学家分享数据。如这篇论文带来了商业机会，相关的权利将会预先被保护起来。我们会在第9章进行进一步的讨论。

区块链合作组织

这个可信的协议促进了合作组织的运作——这是一种由希望实现共同需要的人所组织和控制的自主运作的机构。

“将Uber称为分享经济的说法是荒谬的”，哈佛教授本科勒说道，“Uber使用了移动技术创造一种业务，降低了顾客所需的交通服务的成本。这是已经是Uber所做的一切了。”²⁹戴维·蒂科尔说道，“在英语的平常用法中，分享表明免费的交换，即不存在金融交易，就如孩子分

享玩具一样。很遗憾这个词语已经在一定程度上失去了这个含义了。”对他而言，“事实是，分享就是数百万年来人类和其他生物相互进行交换的方式，分享这个行为自身就对分享下了定义了。互联网公司协助了某种形式的分享，但它们也对分享的行为、词汇和成果进行了商品化，并将其归为己有。”³⁰

大多数所谓的“分享经济”公司实际上是服务的聚合者。它们通过一个中心化的平台将愿意出售闲置资源（汽车，设备，空闲房间，手工艺技能）的供应者聚集在一起，并转卖这些资源，同时收集者宝贵的数据，以用于将来的商业目的。

像Uber这样的公司已经破解了大规模服务聚合和分发的关键。Airbnb（一个服务聚合公司）与酒店进行着旅业的竞争；Lyft和Uber对出租车和礼宾车公司带来了挑战；Zipcar（一个服务聚合公司）在被Avis收购前，用它良好的便利优势及方便的小时费率对传统的汽车租赁公司带来了挑战。

很多这样的公司已经将传统的本地化、小规模的服务（如简易旅馆、出租车和手工艺者）的经营规划变成全球化了。它们使用数字化的技术去利用那些被称为使用率不高的、基于时间分配的资源，如房地产（公寓的床位）、车辆（等待订单中的出租车）和人员（退休人员及不能找到全职工作的人才）。

区块链技术为这些服务的提供者带来了一种相互协作并分享更多价值的方法。对尤查·本科勒而言，“区块链能将人们一起工作的意愿转换到用于记录权利、资产、契约、贡献、使用等事项的可靠的账本中，这样的做法取代了Uber这样的公司所做的某些事情。这样，如果司机们想创立属于他们自己的Uber并用一个纯粹的协作组织取代Uber，区块链让这成为可能。”他强调了“让这成为可能”这词。对他而言，“让这成为可能与将世界推到一个新方向有着不同之处”。他说道，“人们依然需要有

做这件事的愿望，以及为了做这件事承担风险”。[31](#)

所以，为区块链版本的Airbnb、Uber、Lyft、Task Rabbit和各种应用的到来做好准备吧，这些应用会存在于任何有真正地进行分享及以协作的方式进行价值创造并收到他们所创造的大部分成果的地方。

按量计费经济

或许区块链可以将我们带到分享经济之上的一个层次——按量计费经济。我们就可以将闲置的资源出租并按量计费。现实中的分享经济有一个问题，就是房产所有者同意分享电动工具、小型农具、钓鱼用具、木工车间、车库或停车位，但这过程非常麻烦。“在美国，有8000万个电动钻的平均使用时间只有13分钟”，Airbnb的首席执行官布赖恩·切斯基在《纽约时报》的一篇文章中写道，“每一个人都真的需要拥有自己的电动钻吗？”[32](#)

问题是，大多数人觉得自己去家得宝购买14.95美元的电动钻远比花10美元从一英里外（还得算上来回车程）某个人的手中租用这电动钻更简单和更具性价比。Sarah Kessler在《快公司杂志》的一篇文章里写道，“分享经济已经终结了，我们把它杀死了”。[33](#)

不过，通常区块链技术我们可以出租一些特定商品的闲置使用时间，这类商品的分享过程并不存在太多的麻烦事——如Wi-Fi上网热点、计算机运算能力或存储空间、我们的计算机产生的热量、我们闲置的移动电话通话时间甚至是我们的技能——这都不需要做太多的事情，也不用在城市之间的陌生人家中来回往返了。当你去旅游的时候，你的Wi-Fi热点可以无须你的参与而出租自己的上网时间，每秒收取一丁点费用。你的想象力（或者可能出现的新监管政策）是你唯一的限制。你订购的套餐、物理空间和能源现在可以成为一种收入来源，将它们以按量计价的方式卖给对方，并通过微支付手段收取费用。你所需要的只是

一个去中心化的价值传输协议，让其可以安全和可靠地与对方达成交易。这些平台渐渐地往我们的资产里注入衍生权利。你需要决定给别人分配多少使用权和访问权（甚至是防止别人使用你的资产的权利），并考虑这些权利的让渡应该收取多少费用。

这对实体资产来说也是适用的。例如，我们经常听说无人驾驶汽车这个概念。我们可以在区块链上建立一个开放的运输网络，所有者们可以通过一个加密的私钥（数字）去保有一辆汽车。通过公钥基础设施和现有的区块链技术（如Etherlock和Airlock），租车者可以解锁一辆汽车，并在特定的时间段内使用它，这个过程是由智能合约的规则决定的，系统同时会实时对汽车（或其所有者）所消耗的时间和能源进行付款，然后在区块链上进行计量。因为区块链技术的透明性，所有者群体可以跟踪谁在履行承诺。那些不能履行承诺的人将会给其声誉度带来负面影响并最终失去对该系统的访问权。

平台建造者

当企业希望对外界中可能与该企业共同创造价值或新业务的个人或社区开放它们的产品和技术设施时，就会创造平台。其中一个类型是专业消费者（prosumers），这是一种会进行生产的顾客。³⁴在一个有着顾客创新的活力世界里，新一代的专业消费者认为“探索各种新玩法”是他们与生俱来的权力。

区块链技术为产销合一的市场提供了新动力。耐克运动鞋可以在一个分布式账本上生成和存储数据，这样在双方所签署的智能合约的规定下，耐克和运动鞋的用户可以用这些数据实现经济利益。若顾客同意激活鞋子里的智能合约甚至将她的鞋子与其他穿戴用品（心脏监护器或葡萄糖水平计算器或包含其他对耐克有价值数据的设备）同步，耐克可以在每一对卖出去的鞋子里附带一小部分股份。

跟一些与其顾客共同创造产品的专业消费者社区相比较，某些平台具有不同的特点。在开放平台上，一个公司可以为合作伙伴提供更广泛的收入来源，这些合作伙伴需要做的是开创新的业务或简单地为平台增加价值。

现在，通过区块链技术，公司可以快速地创建平台，并与其他人一起合作为整个产业创建平台或实用工具。罗宾·蔡斯是Zipcar和Buzzcar（一个让用户与他人分享汽车的公司）的创始人，他现在是《Peers Inc.》的作者，这本书详细讲述了大众协作所带来的力量。她告诉我们，“若要利用闲置资源里发现的价值，就取决于为鼓励人们参与所设计的高质量平台，这些平台的建造成本并不便宜。区块链在提供标准通用数据库（开放应用程序接口）及标准通用合约方面非常出色。区块链可以让平台的建造成本变得更低、更可控”。这只是一个开始。“它的优势是其通用的数据库有助于提高数据的透明性和可移植性：消费者和供应商可以寻求最佳的条件。他们也可以在区块链上进行相互协作，创造他们自己的平台，而不是使用传统公司的资源”。[35](#)

你可以将汽车看成是未来的一部分。它可以作为基于区块链的网络的一部分而存在，在里面每一个人都可以分享信息，车辆的不同部分可以进行交易和交换金钱。由于有了这样一个开放平台，数以千计的程序员和小众商业可以为你的汽车定制应用。很快，这样的平台可以通过执行各种金融交易和价值交换的结算而为金融服务等产业带来转型机会。一个由各家大型银行组成的联盟已经在探索这个思路了。平台在产业中扮演着重要的角色。

《维基经济学》讲述了创意集市的概念，这是一种为创意、发明、独特的人才而设的新市场，保洁这样的公司在里面利用的高技能人才的规模是它自身雇员的10倍之多。一些公司使用像Innocentive和Inno360这样的服务去实施“挑战任务”、“数字化头脑风暴”和其他的技巧，以在公司的边界外寻找合适的临时性人才，从而解决关键的业务挑战。这是关

于如何使用数据去寻找合适的人才从而更好地解决业务中存在的问题。

人才——那些有着解决问题所需的、有着独特思维方式的人可以在分布式账本上张贴自己的求职信息，这样公司可以找到他们。现在我们希望用bInnocentive去代替Innocentive这种服务。人们可以创造可流动的身份和简历（有关他们身份信息的详细版本），可用于向潜在的雇佣者提供有关自己的合适信息。你可以将这个系统看成是一个无人拥有的分布式技能数据库。

随着每一种商业模式都变成一种数字化商业模式，黑客马拉松是创意集市的一种重要形式。现在，通过区块链技术和开源代码库的使用，每一个公司都可以向极客（geeks）和其他业务创造者提供解决问题、创新和创造新商业价值所需的场所。

区块链与基于区块链的软件库将会对这样的活动提供帮助。现在，公司可以使用如以太坊区块链这样内置支付系统的新型、功能强大的编程语言。摘自《黑客新闻》里的一个对话的片段是这样的：“想象一下这样该多好——如果我能分享我的程序库里的全局唯一标识符，这样你的bit客户端（可以称为gitcoin或bit）可以从分布式区块链（实质上是git日志）上获取新提交的代码。Github不再是一个中介了，也不会再存在单点失效（single point of failure）的可能性。如果你的程序库需要保密，那就不要对外分享其全局唯一标识符就行了”。[36](#)

区块链上的制造业

制造密集型产业可以创建一个为实体商品的外包、设计和生产而设的全球生态系统，这标志着全球生产会进入一个新的阶段。现在我们讨论的话题是如何在区块链上实现这个生态系统。就如现代飞机被称为“一堆以编队形式飞行的零部件”，在大多数产业中的公司也开始变成由供应商和合作伙伴组成的网络。三维打印技术缩短了用户与生产环节

的距离，给大众化定制带来了新的生命。很快，数据和权利持有者可以将从人类细胞到铝电池在内的任何物质的元数据存储到区块链上，这样将会解除公司生产环节所面临的局限。

这项技术也可以用于对供应链网络中的商品的起源及其流转过程进行深入的观察。我们来思考一个与我们生活息息相关的产业，即食物产业。现在，你当地的杂货店或许会声称（而且它们或许真的相信）它所售卖的牛肉是安全的、以人道的方式喂养的、喂食了合格的饲料并且没有添加任何非必要的药品。不过它无法证明这些事情。没有人会为每一头牛的历史进行记录；健康的牛也会发生不好的事。我们在缺乏验证方法的情况下只能信任我们的汉堡包的安全性。通常来说这对我们并没有什么区别——这类食品还是在不停地大量供应。不过偶尔我们会看到疯牛病的迹象。

食品产业可以在区块链上储存每一个运输过程的编号、每一份肉，还有可能与其DNA关联起来。三维搜索能够详细地追踪牲畜和家禽的流转过程，这样用户可以将一只动物的身份与其历史关联起来。通过复杂的基于DNA的技术（但相对来说容易使用的）及智能数据库管理技术，即使是最大的肉类供应商都可以确保其质量和安全性。想象一下这些数据有可能加速实验室测试和社区对卫生危机的响应。

这种希望了解我们的食物是怎样喂养或种植出来的这种想法并不激进。我们的祖先在本地的市场或从在本地采购产品的零售商手中购买物资。如果他们不喜欢本地的某个农场主对待其牲畜的方式，他们就不从他手上买牛肉了。不过运输过程和冷藏设备将我们与食物分离开来了。我们失去了旧的食物链中的某些价值。

我们可以恢复这些价值。我们可以带领世界去开发一个现代化的、产业化的、开放的及符合实际家庭农场价值观的开放式食物系统。透明性让有着更高运作水平的公司能够突围而出。而公司的品牌可以从市场的某种“信任标志”的市场营销概念（顾客之所以相信它是因为这是很熟

悉的)进化成基于透明性的关系。食物生产商对此肯定感兴趣。[37](#)

企业协作

尤查·本科勒提及了区块链技术能如何辅助公司内及公司与各种群体之间的协作。“你能有一个为各种事情而设的会计、行动、数字化资源管理的分布式机制,不管它是货币、社会关系和交换或一个组织。这个主意让我感到很兴奋”。[38](#)

现在,商业化的协作工具正开始改变知识性工作和组织内管理工作的性质。[39](#)像Jive、IBM的Connections、Salesforce的Chatter、思科的Quad、微软的Yammer、Google工作应用套件和Facebook工作版这样的产品正被用于改善绩效和鼓励创新。社交软件将成为一个重要的工具,被用于业务运作每一个环节的转型——从产品开发到人力资源、市场营销、顾客服务和销售,这是21世纪的组织的新操作系统的概念。

不过,现在的工具套件还是有着明显的局限性,而区块链能将这些技术带到下一个阶段。现有的供应商可能会面临巨大的挑战,或许他们会拥抱区块链技术并为顾客带来更多的福利。

为公司而设的区块链社交网络是什么样子的?你可以将它想象成为公司而设的Facebook(或大众使用的Facebook的一个替代品)。现在已经有几个公司在开发这样的项目,所以我们可以预测一下在未来一两年内可能发生的事情:

每一个用户都会有一个多功能的钱包,就像是一个进入去中心化在线世界的入口。可以将这看成是一个你所拥有的、可流动的个人档案、人格或身份。与你的Facebook档案不同的是,这个钱包有不同的功能,可以储存各种身份和专业的数据,以及包含货币在内的有价物品。你可以确保钱包的隐私性,并只对外分享你所选择的信息。你会有一对公钥

和私钥，可用于管理你的长期数字身份。虽然一个钱包可以为每一个人或公司存储多个身份，但我们可以先假设一个钱包保存着一个单一的正规身份，这个身份是与一对公钥和私钥的组合绑定的。另外，还有一个发布系统可提供你或你的公司愿意支付的信息流，这可能是如下的内容：一个同事给一份新代码写的补丁、与一个新客户所发生对话的总结、在客户许可下提供的电话录音、一个你无法参与的会议上的推特信息、客户使用你的新产品时的直播视频、你的竞争者在一个产业博览会展台上的照片、一个看似是在达成新业务协议的简报材料、一个同事的新发明相关的视频教程、完成专利申请所需的帮助及其它你认为重要的事情。

另外，还有广告，或许是来自第三方或来自人力资源部门有关职位开放或保险计划修改的信息，但当你付出注意力后，是你（而不是Facebook）会得到收入或某种形式的回报。这被称为“注意力市场”。你有可能因为如下的事情而获得微小的报酬：同意观看一个广告或与之进行互动，或关于新产品推广材料的反馈意见，或任何事情——如帮别人转录验证码⁴⁰或扫描文档。

新闻流、发布系统和注意力市场看上去很相似，不过其支付流则有所不同。ConsenSys的约瑟夫·卢宾说道，“你为发布的内容付款。公司为你注意力付款。新闻流里面没有支付流。我会很高兴地阅读你的信息流，因为我重视社交关系，但我不会付款去看一张你和你的伙伴们在酒吧喝酒的照片，或付款去了解你对Blue Jays球队先发投手的看法”。⁴¹

另外，还有一些灵活的机制能用于寻找你可能关心的人或信息来源。还有，分布式工具为你聚集和展示新的人或信息，让你可以与之成为朋友或跟进该信息，甚至可以利用Facebook的社交图表。约瑟夫·卢宾将这种做法称为“通过使用中心化网络的支柱去构建去中心化的网络”。⁴²

经验表明，在数字时代，有价值的东西始终能胜出。至少对用户和公司而言，这个分布式模式的优点是很显著的。虽然社交媒体公司有着庞大的资源，但我们在这样的一个开源环境中可以实现的丰富程度和功能是没有尽头的。若你将Linux的力量和成功程度与专有的操作系统相比就明白了。区块链技术确保了安全性。你的隐私保护参数完全是可以进行配置的。除非有你的许可，否则没有社交媒体公司可以售卖或泄露你的个人信息。由于你拥有你的数据，你可以用你的注意力和付出去获得经济利益。你可以分享到大数据所创造的财富。

若公司的员工开始在业务中使用这样的平台，公司也应该感到高兴。为了吸引人才，公司应该展示出其正直性，并尊重员工的安全性和隐私。更主要的是，随着企业的网络化并在公司外寻找人才，公司可以贡献出这样的一套企业间协作平台，让合作伙伴可以信任它。时间会说明一切。

概括地说，无论什么规模的公司都能将七种新兴的商业模式放到区块链上发挥功能。总的来说，开放式联网企业在以下这些方面展示出了深远甚至是重大的潜力：促进创新及利用杰出资源，从而为股东、顾客和社会创造良好价值。

改变你的未来：商业模式创新

现在有了由软件代理人管理的公司这个概念，罗纳德·科斯必定在经济学家天堂（有的人或许想说这个地方不存在）的某处对此击掌相庆了。还记得科斯定理的相反面吗？即一个公司的规模应该持续缩减，直到其内部交易成本低于其外部交易成本。在市场上，技术让成本变得更低了，可以想象的是公司可以并应该保有较少的内部规模（软件和资本除外）。

想一下这个情况吧。

首先，搜索的成本会持续下降，这是因为新的代理人可以在登载所有（存在或曾经存在的）商业信息的世界账本上进行三维的搜索。所以若要获取与运营商业相关的信息，就不再需要涉及公司图书馆、信息专家、人力资源搜索专家或无数的其他专家了。

其次，智能合约会极大地降低合约签署、管理及支付的成本。不再会有纸质的合约了，这些程序可以通过一系列的模板制定其条款；还可以基于从外界收集到的规则和详细信息，进行讨价还价，并接受或拒绝对方提出的条款与条件；制定自我执行的政策；决定表现条件是否已经被满足了；还有执行交易。

第三，在公司之外协调这些资源的成本可以忽略不计——可以表现为驱动部署了企业软件的服务器所需的能源。至于对企业所雇佣的人类、组织或工厂的管理而言，企业并不需要官僚主义的制度。通过这个新的平台，我们可以想象出一种新型的机构，它需要很少（甚至不需要）传统的管理制度或层级机制，也能为顾客带来价值及为所有者创造财富。

最后，建立信任的成本可以接近于零。信任不依赖于该组织，而是依托底层代码的功能、安全性和可审计性及无数在维护区块链安全性的人所构成的大规模协作行动。

你会如何设计一个分布式的自主运作企业？这样的—一个实体将会有丰富的功能——代理人会基于一个预先批准的章程执行一系列的任务或更广阔的商业职能。个人、组织或潜在股东、用户所构成的集体将会通过定义如下的内容进行设计：

1.决心：有关对世界及创造价值、改变事物所需完成的事情的信仰。

2.用途：它存在的原因。我们为什么要创造这样的企业呢？

3.章程：描述企业的总体目标及其用于价值的创造所对应的规则。

4.做法：例如，它会如何创造这种价值。它会如何资助自己的活动——通过众筹、传统的早期投资或使用其收入。它会如何获取各种资源？

5.人类与技术之间的分工。在可以预见的将来，或许人类应该处于负责的位置。

6.应用功能：企业将如何探测并回应情况的改变。

7.道德准则：Google的“不作恶”承诺并不足够。这个去中心化的自主运作企业需要有清晰的准则去定义什么是（还有什么不是）可以接受的行为。

在近期，可能不会出现分布式的自主运作企业，不过若对这些新的实体进行预先的思考和调查，可以为你今天的商业策略的制定提供帮助。这个为身份、信任、声誉度和交易而设的全球点对点平台的兴起，我们终于可以改变公司的底层架构，从而促进创新、共享的价值创造甚至是为多数人创造的繁荣，而不只是为少数人创造财富。现在，你能看到最少有7种新兴的商业模式，可以在你的产业内带来冲击，同时以新的方式进行财富的分配。

总的来说，聪明的公司将会努力参与到区块链经济里，而不是扮演受害者的角色。在发展中国家，价值创造的分配（通过企业家精神）和价值参与（通过分布式的公司所有权）或许是解决繁荣悖论的关键。若考虑到数十亿的自主运作的代理人将会被嵌入到现实世界中，我们的故事就变得越来越有趣了。这就为我们带来了第七章的内容。

第六章

万物账本：物理世界的活化

在一个很热的晚上，澳大利亚某处偏远内陆地区的一根电线杆在8点整倒下来了。这对在维多利亚大沙漠边缘的一个以金矿为主业的老镇Laverton以外100英里的地方圈养了一些绵羊和牛的威廉和奥利维娅·芒罗来说是一个问题。¹在这个夏天，气温经常会飙升到48.9℃摄氏度。他们的孩子Peter和Lois通过卫星链路完成学习，而这也是这个家庭在生病或出现紧急情况时用于与外界卫生服务联系的途径。虽然芒罗一家有一个后备发电机，但它不能长时间驱动水泵、通信和空调设备。总之，芒罗这一家人的生活完全依赖于可靠的能源。

在9小时后的黎明，电力公司派出了一个团队去寻找和修复倒下的电线杆。客户的投诉让公司对故障发生的地点有个大概的想法，但这个团队花费了超过一天的时间去识别、寻找和修复这条电线杆。同时，芒罗一家和附近的居民、商业和机构失去了电力和与外界通信的途径，这带来了极大的不便，还带来了经济损失和健康风险。在内陆地区，停电不只是让生活停摆，而是很危险的。为了让这些危害最小化，电力公司花费了很高的成本派遣检查员定期去检查庞大的电力网络，试图发现倒下或老化的电线杆。

想象一下若每根电线杆都是一个智能设备，那么它的维护工作就变得更安全、简单和廉价了。它可以对自身的状态进行汇报并传召相关人员进行替换或维修。无论是什么原因，若一根电线杆发生火灾或开始倾侧、倒下，它会实时生成一个事故报告并通知维修队带上合适的设备来到一个详细的地点进行修复。同时，这条电线杆可以将自己的任务重新指派给附近正常工作的电线杆。毕竟，它们是在同一个输电网中。公共事业公司可以更快速地为社区恢复电力供应，而无须现场勘查所需的庞

大、持续费用。

为人们提供电力

这仅仅是一个开始。通过使用与物联网相关联的新兴软件和技术，我们可以将智能的元素逐渐地注入现有的基础设施里，如输电网也可以加入能够彼此通信的智能设备。想象一下，如果能够快速地创建一个全新的灵活、安全的网络，而且具备较低的成本，能够为新服务、更多参与者及更高经济价值的实现带来更多的机会。

这样的结构被称为网状网络（mesh network），即一个将电脑和其他设备直接连接到一起的网络。它们可以根据带宽条件、存储空间和其他能力自动进行重新配置，因此可以抵御故障和干扰。缺乏网络访问条件或可负担服务的社区可以使用网状网络维持基本的网络连接。网状网络是传统的机构、监管和控制从上到下的模型的替代方案；它们可以提供更高的隐私保护和安全性，因为信息流并不会经过一个中心机构。²

一些机构已经在将网状网络与区块链技术结合起来，以解决复杂的基础设施问题。美国的一家物联网公司Filament正在澳大利亚内陆地区进行一项实验，涉及一种名为“tap”的设备，可以用于电线杆上。这些设备可以直接在相互之间通信，距离最远可达10英里。由于电线杆之间的距离大概是200英尺，因此若当一根电线杆倒下时，上面的一个动作检测器就会通知200英尺外的另一根电线杆并告诉它“我有麻烦了”。如果另一根电线杆上的tap设备出于某些原因无法联系上，那么它会继续联系下一条电线杆，或者是联系下一根（最远可达10英里）能通过最近的互联网回程连接位置（120英里内）与公司联系的电线杆。

这个tap设备上有着可以持续20年的电池以及低能耗蓝牙技术，顾客可以将这个设备直接连接到他们的手机、平板设备或电脑上。这个

tap设置内置了很多传感器，可以检测温度、湿度、光强度和声音，这样顾客就可以用来监测和分析一段时间内的状况，或许还能开发出预测性算法，从而预测一条电线杆的生命周期或即将发生的故障。顾客可以成为气象节点，或将这些数据作为一种信息服务，或将这些数据集在区块链上授权给另一个用户（如政府、广播公司、电线杆制造商或环保机构）。

Filament的商业模式是一个涉及了三方的服务模式：Filament、它的集成业务客户及公共事业公司。Filament拥有硬件；它的设备持续地监测电线杆的状况并汇报情况的改变——不管是倒塌、发生火灾，还是因为粉尘积聚或山林火灾烟雾所造成的故障。Filament将传感器数据流售卖给集成业务商，而集成业务商转卖给公共事业公司。

公共事业公司每月为这样的监测服务支付费用。这样的服务使得电力公司无须再进行成本极高的现场勘查工作。由于电线杆在极少数的情况下才会倒下来，电力公司也很少使用网状网络的实际通信能力，这样Filament可以将这些tap设备的多余能力部署给其他的用户。

“由于Filament拥有这些设备，我们可以将这个横跨大陆大部分地区的网络之上的闲置网络处理能力卖出去”，Filament的联合创始人及首席执行官埃里克·詹宁斯说道，“Filament可以与FedEx快递公司达成协议，通过我们在澳大利亚农村地区的网络让它们的中型卡车有能力实时地往总部发送遥感数据。我们将FedEx加入到智能合约的列表中，现在它们可以付款给每一个设备，让这些设备向他们发送数据”。³FedEx的司机们可以使用网状网络作为通信和车辆跟踪的手段，以在偏远地区指示预计的到达时间和各种故障情况。若故障情况发生了，网络就会向最近的维修工厂发出警报，让它们的维修队带上必需的零件和设备来到故障现场。

区块链技术是很重要的。这个物联网的应用依赖于万物账本

（Ledger of Things）。成千上万的智能电线杆通过很多的传感器收集数据并将这些数据传递给其他设备（计算机或人），这个系统需要持续地追踪所有事物，这包括能够识别每一根独特的电线杆的能力，以确保其可靠性。

“如果没有身份的话，其他事情也没法实现了”，埃里克·詹宁斯说道，“区块链上的身份是物联网的核心。我们为每一个设备都创建了一条独立的通道。这条通道和身份随后会存储在比特币的区块链上（特定的位置是分配给了Filament）。就如比特币一样，它可以被发送到任何地址”。⁴区块链（及智能合约）也确保了设备的费用已经有人支付了，这样它们就可以继续工作。离开区块链支付网络的话，物联网就无法发挥功能，比特币在这其中是通用的事务语言。

社会能源：为街区提供能源

现在，除了电线杆外，想象一下你可以将电力系统里面的所有节点进行数字化，以创建一个全新的点对点能源生产和分配模式。每一个人可以参与到一个由区块链驱动的供电网络。在纽约州赞助的一个提高能源体系可靠性（哪怕是在极端天气的情况下）项目里，它们已经开始在布鲁克林Park Slope地区创建一个社区微电网了。当它建成后，这个微电网和它本地生产的电能将会在紧急情况时提供应急能力并为顾客降低成本，同时在社区中促进清洁的、可再生的电力、能源效率及能源储存选项的探索。

虽然校园内的微电网已经出现一段时间了，但它在居民区并不是很常见。北美的城市区大多数的房屋所有者、商业、政府和其他机构从固定的公共事业公司以固定的价格购买电力。现在，我们有不少坐落在本地的可再生的能源选项，如屋顶上的太阳能电池板。本地的公共事业公司会以批发价（通常会有不少的折扣）采购这个太阳能电池板生产的过剩电力。一个顾客可能就是在本地的能源生产者对面的房子里居住，但

他们依然需要经过公共事业公司并为自己邻居生产的可再生能源支付完整的零售价。这是很荒谬的事情。

“现在的公共事业公司有一套命令和控制系统，由少数人去运营一个公共电网。与此不同的是，你可以设计让公共电网负责自身运营的机制”，罗山能源公司的联合创始人及负责人劳伦斯·奥尔西尼说道，“随着公共电网中的节点中的所有资产都帮助维护和运行这个电网，网络的恢复能力就更强了”。⁵这是一个通过在资产里嵌入智能合约及其它控制机制而实现的分布式的点对点物联网网络模型（如区块链模型）。⁶当一场飓风摧毁了输电杆塔或火灾损害了一个变电站，这个公共电网能够快速、自动地重新分配电力，以避免大规模的停电。

恢复能力并不是唯一的好处。在本地使用本地产出的电力比公共事业公司的大规模输电网要高效得多，后者需要在远距离传输电力，这样会带来电力的损耗。罗山能源公司正与当地的公共事业公司、社区领袖和技术合作伙伴一起创建一个市场，在里面，邻居们可以买卖具有环境价值的能源。“因此，你不需要付费给一个采购了可再生能源额度的能源服务公司，而是直接付费给那些真正地在生产出你家中所使用的电力的人，这样的模式是本地化的、绿色的，对你的街区来说也有环境上的意义。这看上去是更公平了，对吗？”劳伦斯·奥尔西尼说道。⁷是的！

如果你可以定位每一个这样的资产并为生产和消费分配一个区位价值，这样你就能创建一个实时的市场。根据劳伦斯·奥尔西尼所说的那样，你可以将多余的能源向也在生产可再生能源的邻居进行拍卖。这样做的话，你的社区可以通过点对点交易实现能源供应的可靠性。社区成员可以就实时微电网市场的规则达成共识，如时间段计费、最低价或最高价、离你最近的邻居的优先度或其他用于优化价格及实现最少浪费的参数。你将不需要整天坐在电脑前进行价格的设置或提出购买、售卖的提议。

未来的微电网将可以收集它们的计算能力所创造出来的热量，将东西加热，捕捉和储存这些热量，这样节点自己可以生成非常小额的电力，人们就能在家中的微电网使用这些电力了。将计算能力分配到社区的建筑物中并使用所产生的高温去驱动供暖、热水和空调系统的方法，可以提高同样的能源的生产力。“我们的关注焦点是提高最大的效能。”劳伦斯·奥尔西尼说道。

随着本地化生成的可再生能源越来越多，物联网对固定的公共事业模式提出了挑战，这并不是很遥远的事情了。我们需要应对气候变化并准备好迎接极端气象条件所带来的挑战，特别是把海洋中的岛屿淹没的雨、让旱地变成沙漠的旱灾。现在，我们每年因沙漠化要失去1500万英亩的土地，情况最坏的是在撒哈拉以南非洲地区，在那里人们无法像位于澳大利亚内陆地区的芒罗一家那样负担水泵、空调或迁移的费用。⁸ 我们需要输电网络和引擎不再把能源和二氧化碳排放到大气层中。现在公共事业公司正在评估将物联网整合到其现有基础设施能所带来的好处（“智能电网”），若能连接到微电网将会带来一种全新的能源模式。公共事业公司、它们的工会、监管者和政策制定者及像罗山能源公司这样具有创新思维的新成员正在探索这样的新模式：首先在街区的层面生产、分配及使用电力，然后再到全世界。

计算机的进化：从大型主机到智能药丸

与我们的能源网络不一样的是，计算能力已经通过几个范式得以进化了。在20世纪50年代至60年代，大型计算机是主流，其中的代表有IBM、Wild “BUNCH”（Burroughs、Univac、国家现金出纳机公司、Control Data和Honeywell）。在20世纪70年代至80年代，微型计算机登上了舞台。Tracy Kidder在他的畅销书《新机器的灵魂》一书中预测了通用数据（Data General）的崛起。就如大型计算机的公司一样，这些

公司中的大部分已经退出了该业务或消失了。谁还记得数字设备公司、Prime Computer、王安电脑、Datapoint或惠普、IBM的微型计算机？在1982年，IBM的硬件和微软的软件给我们带来了个人电脑的时代，而那时候苹果公司的Macintosh微型计算机还无法与其竞争。这就是时代的变迁。

通信网络也随着同样的技术进步而进化了。从20世纪70年代的早期开始，互联网（起源自美国的高级研究计划署网络ARPANET）进化到了它现时的状态——世界范围内的分布式网络，将超过32亿⁹的人口、商业、政府和其他机构连接在一起。计算机技术和网络技术然后又融合成了移动平板和手持设备。黑莓（Blackberry）在21世纪早期将智能手机商业化了，而苹果公司在2007年通过iPhone让智能手机流行化了。

这其中相对来说较新颖和令人兴奋之处是这些设备的能力已经超越了被动式的监视、测量和通信（气象模型、交通模型）、传感探测和响应；它已经进化到可以根据预先定义的行事规则执行交易或任务。它们可以感知（温度的下降或交通堵塞）并进行响应（给火炉点火或延长绿灯时间）；测量（动作、热量）和通信（应急服务）；定位（爆裂的总水管）和通知（维修队）；监视（位置，临近）和变化（方向）；识别（你的存在）和瞄准（向你进行营销），以及实现其他的一些可能性。

这些设备可以是静态的（电线杆、树和管道）或动态的（衣服、头盔、车辆、宠物、濒危动物和药品）。护理人员正使用智能（或可食用）的电子药片以识别和记录病人的服药时间。一片皮肤贴布或覆盖物能够捕捉数据并测量心律、食物消耗量或其他因素并将此信息通过一个能够识别特征并给做出反馈的应用程序发送给医生、护工或病人自己。医药界很快将会使用类似的技术，用于特定癌症的定向给药、测量体温及其他生物指标。¹⁰

这些设备可以在相互之间进行通信——直接与计算机或数据库通

信，或通过云端服务器进行，而且与人通信（向你发送一条短信息或拨打你的移动电话）。通过不断进化的机器智能和所收集的数据，这些设备正将数据的分析、特征的识别及趋势观察这些任务放到每一个人的手上。¹¹产业里的术语“大数据”远远不足以描述现实世界将会产生的海量数据。据最保守的估计，今天100亿左右通过互联网连接起来的设备将会在2020年增加到250亿。¹²考虑到这是来自无限数量的设备，将其称为“无限数据”可能更合适。

那么，为什么我们还没有居住在智能家居里、驾驶智能汽车和使用智能药物？我们看到了6个主要障碍。其中一个是一些小题大做的应用程序和服务的推出。简单地说，早期的消费者物联网设备很少有带来实际价值的——除非你认为让你的烟雾探测器命令你的夜灯打电话给你的智能手机并给你发出火警警告算是一种价值。¹³

另一个障碍是来自高管们、产业协会和工会无法预见新的策略、商业模式和人们的角色，这主要是因为组织惰性、不情愿或无法去做这些事情。一些有创新精神的企业家已经根据这样的一些原则开发了新的商业模式（如让实体资产可以被识别、搜索、使用和付款），因此也对现有的市场带来了冲击（如Uber和Airbnb），不过其冲击相对来说还是很小的，而且依赖于一个公司及其APP充当中介的角色。

第三个障碍是对恶意黑客或其他安全漏洞会改变信息和行事规则并绕过安全机制控制设备从而带来潜在的灾难性后果的忧虑。

第四个障碍是“产品未来寿命”所带来的挑战，这对那些有着很长生命周期的资产来说是一个问题——这些资产的生命周期远比一个典型的应用程序或一个公司的要长得多。初创企业经常出现破产或将自身出售给更大规模的公司情况。

第五个障碍是可扩展性。若要实现物联网的全面价值，我们必需能

够与多个网络进行连接，这样它们才可以进行相互操作。

最后一个障碍是中心化数据库技术首要的挑战——它无法低成本地处理上万亿的实时交易。

若要解决这些障碍，万物联网需要有万物（机器、人、动物和植物）账本。

物联网需要万物账本

欢迎来到由万物账本驱动的万物联网——得益于区块链技术，在互联网中将会实现的分布式、可靠的、安全的信息分享、传感和自动执行动作及交易。技术专家和科幻小说作者一直在想象由与互联网相连的传感器所构成的无缝全球网络可以捕捉地球上的每一次事件、动作改变。通过无处不在的网络、持续进化的处理能力以及廉价、小型联网设备的不断出现，物联网的愿景越来越接近现实了。

记住中本聪对比特币区块链的设计是要确保每一个在线的比特币交易的完整性以及比特币这个货币的整体运作。通过在每一个节点上记录每一笔交易，然后与网络（区块链）中的每一个节点分享这个记录，我们可以快速、无缝地在点对点网络中验证交易。我们可以执行有价值的交易，在这个例子里是金融的交易，这种模式是自动化的、安全的、机密的，而且无须认识或信任网络上的每一个节点，或无须通过中介。万物账本对信任关系的依赖程度是很低的。

区块链技术让我们可以将相关的核心信息与智能设备关联在一起进行识别，并对其进行编程，使得它能够在预先定义的规则下执行动作，而无须担心错误、篡改或在澳大利亚内陆地区被关闭的风险。因为区块链是一个不可干预的账本，上面记录了网络中发生的所有数据的交换记录，这些记录在运行中不断进行积累，并由该特定网络中的协作节点进

行维护，这样用户可以确保这些数据是准确的。

越来越多的技术公司认为区块链对释放物联网的潜力至关重要。大型、中心化计算机系统的始祖IBM恰恰开展了相关的研究。在一份题为《设备民主：拯救物联网的未来》的报告中，IBM指出了区块链的价值：

“在我们的去中心化物联网的愿景中，区块链是在发生互动的设备间促进交易处理和协作的一个框架。每一个设备管理着自己的角色和行为，这就带来了‘去中心化、自主运作的物件的联网’——因此走向了数字世界的民主化。设备可以自主地执行数字合约，如通过搜索自己的软件更新、验证节点的可信性、支付和交换资源及服务，从而与各个设备建立协议、支付和贸易关系。这让它们能够以自我维护的、自我服务的设备形式运行。”¹⁴

因此，区块链的使用开启了全新的商业模式，因为网络上的每一个设备或节点可以作为一个独立的微型商业主体运行（如低成本地分享电能或计算能力）。

“其他的例子有音乐服务或无人汽车”，智能钱包公司创始人迪诺·马克·安格里蒂斯说道，“我需要对每一秒的播放音乐或乘车的需求进行付费——从我的账户余额中扣去一分钱的几分之一。我不需要预先付很多钱，而且只需要为我使用的服务付费。供应商不必担心我不付款。你在传统的支付网络里无法实现这些事情，因为从你的信用卡上扣取一分钱的几分之一的手续费太高了”。¹⁵

多余的卧室、闲置的公寓或会议房间可以自己出租自己。专利技术可以自己为自己申请证书。我们的电子邮件可以对所收到的每一封垃圾邮件的发送者进行收费。你应该明白这个想法了。通过机器学习、传感器和机器人，自动运作的代理人可以管理以下的事物：我们的家居和办

公楼、交互式销售和市场营销、公交车站的棚子、车流量及道路使用情况、废物收集和处理（垃圾桶与垃圾车交流）、能源系统、供水系统、内嵌或穿戴的医疗保健设备、库存、工厂与供应链。

WISeKey的首席执行官卡洛斯·莫雷拉认为产业区块链里有着巨大的机会。¹⁶WISeKey是一个位于瑞士的公司，研究领域包括身份管理、网络安全和移动通信，为手表和其他穿戴设备提供安全的交易处理能力，现在正向生产商和芯片制造商提供其信任模型，这种模型能为大量的物联网设备提供验证功能，并让它们通过互联网或其他网络进行通信。“我们现在正进入另一个世界，在那里信任是在物体的层面授权的。一个不被信任的物体将会自动被其他物体拒绝，而无须事先询问一个中心化的权力机构”，卡洛斯·莫雷拉说道，“这是未来几年可能会给流程处理带来深远影响的重大范式转型”。¹⁷

在这个新兴的世界，用户使用安全的身份验证和校验（还可能有公钥/私钥）与其他智能合约连接起来，然后与其他设备定义事务处理规则（如隐私性）而不是执行某个中心化节点或中介机构设定的规则。生产商可以将维护、所有权、访问权和责任转移给由自我维护的设备组成的社区，让物联网可以在将来得以发展，并节省基础设施成本，并精确到在每一个设备老化的时候替换它。

因此，区块链可以解决一个可持续的物联网面临的6大障碍。概括地说，万物账本有9个很好的网络特性：

可恢复性——自我纠错；没有单点失败的风险

处理能力强——可以处理数十亿的数据点和交易

实时性——全天候运作，数据实时流动

响应性——能够对变化的状况做出回应

极度的开放性——持续地根据新的输入而进化和改变

可再生——可以是多重用途的、重复利用及回收过的

简化性——成本和摩擦最小化，处理效率最大化

产生收入——创造新型的商业模式和机会

可靠性——确保数据完整性，参与者的可信性

我们为什么相信由区块链驱动的物联网有这样的巨大潜力呢？主要的原因是它能够让物理世界充满“生机”。一旦我们在区块链上为这些物体赋予“生命”，它们可以感知、响应、通信、和执行操作。根据智能合约的规则，资产可以搜索、寻找、使用和补偿其他的资产，从而让一个有着高度颠覆潜力的新市场成为可能，这就像之前互联网为人们和各种数字内容所提供的驱动作用一样。

对管理者、企业家和民间领袖来说有一个问题：你该如何利用这些新机会去执行改变和实现增长？你的组织将会如何响应对你现有运作模式来说不可避免的颠覆？你将如何与初创企业和协作组织的创新性新模式竞争？

在我们的生活中，更高的效率、改进的服务、降低的成本、提高了安全性和更好的结果充满着不少的实现机会，而我们可以通过将区块链的逻辑应用到物联网上的方式改善上述目标。我们开始了数字化革命的下一个主要阶段。英特尔公司的米歇尔·延斯利解释了她的公司正深入调查区块链革命的原因：“当个人电脑变得无处不在时，生产率达到了前所未有的水平。我们将那些个人电脑连接到一个服务器、数据中心或云服务器，让小型的初创企业可以方便地获取计算机资源，现在我们再次看到了飞速的创新和新型的商业模式”。¹⁸英特尔希望加速对各种模式的优劣及其中所存在的机会的理解过程。“我们可以预期这个技术将会

带来一个全新的创新功能，能为各种新公司、新参与者提供驱动力。作为产业里的领导者之一，我们不能在这场对话中缺席”，她说道。¹⁹你可以想象一下将这些潜能应用到各种类型的商业上——其中的很多还未被互联网革命影响过。

12个颠覆的领域：物理世界的活化

让物理世界活动起来，这会产生什么可能性？与匹诺曹（《木偶奇遇记》主人公）不一样的是，我们并没有一个蓝衣仙女。（而且，与匹诺曹不一样的是，区块链不会撒谎。）不过，今天，现在我们有分布式账本技术，它将不仅会让通用电气的“带来美好生活”的口号成真，而且匹诺曹也无法对账本撒谎了。

我们还处于想象万物账本（嵌入到物联网中）各种可能性的早期阶段。直至今天，流行媒体关注的焦点还是消费类设备，不过万物账本在每一个领域都有潜在的应用。对潜在应用的分类和分组有着很多的方法，因为各种跨界的应用可以被归纳到超过一种类别里。例如，麦肯锡公司在它对物联网的分类里使用了集合的概念。²⁰我们已经界定出万物账本中所存在的机会，并划分为12个主要的功能领域。这里面的特定的好处以及商业案例对每一个应用来说都是具体的。下面的类别分类描绘了其潜力及对现有的市场、参与者和商业模式可能带来的显著影响。

运输

在未来，你将可以召唤一台无人驾驶汽车并将你安全地送达目的地。它自己会选择最快的路径，避开施工地段，处理道路收费站相关事项并自己泊车。在交通堵塞的时候，你的车辆会计算出道路的通行率，这样你可以及时地到达目的地，而货运的管理者将会在所有的货物上使用基于区块链的物联网设备，以快速通过海关或其它所需的检查项目。

这样，不会有条条框框的限制。清道车生产商Allianz可以将其市政设备装上迷你摄像头或传感器技术，以鉴别那些在纽约将车辆停泊在停车区的另一边并几天没有开走（如果它们无法自己开走）的情况，然后将传感器数据发送给交通警察，这就省下了书写实物的违规停车罚单的过程。或者，清道车自己可以在经过车辆的时候以比特币的形式直接从违规车辆中进行罚款，因为纽约州的运输部门到时候可以要求所有的车辆在纽约的5个区域进行注册，并保持一个与他们的车牌相对应的比特币钱包地址。在另一方面，无人驾驶汽车则可以感应到正在驶来的清道车并轻松地开走，以让清道车经过。

基础设施管理

很多专业人士会使用智能设备去监控人行道、铁路、电线杆和电线、管道、港口和其他公共和私营的基础设施的地点、完整性、年限及其他相关的因素，以快速、低成本和高效低监测状况、发现问题（如损坏或被破坏）并做出响应。这就是像Filament这样的公司的业务领域，它们利用可负担的科技去改造现有的基础设施，为其带来新的生命周期，而无须替换基础设施所需的巨额资金。Filament的埃里克·詹宁斯预计“超过90%的基础设施当前并没有被连接起来，若要将这些现有的设施都拆除并替换成全新的无线互联资产，显然是不现实的”。²¹

能源、垃圾和供水管理

已经装满了垃圾的垃圾桶说：“请派一辆车来运走我的垃圾。”渗漏的水管说：“把我修复吧。”围绕物联网展开的想像力带来的灵感，应该能启发产生许多新的儿童书籍。在发达国家和发展中国家，传统的公共事业公司可以使用基于区块链的物联网以实现追踪生产、分配、消费和收集。就如我们已经看到的那样，那些没有投入大量基础设施的新竞争者正计划用这些技术创建全新的市场和模式（如社区微电网）。

资源开采和农业

区块链也可以用于牛的溯源管理上，让农民可以追踪它的食物、给药记录及完整的健康历史。这个技术也可以帮助追踪昂贵的、高度定制化的设备，并让它在更广泛的地方能够及时地满足需要，并收回成本；也可以通过对标记安全设备的标记和自动化的检查清单（以确保设备被合适地使用）提高矿工和工人的安全度；通过对天气、土壤和农作物状况的监测进行灌溉、自动化收割或其他操作；基于历史上曾经出现的模式和结果，对“无限数据”进行分析从而发现新的资源或为农业生产的运作提出合适的建议。安装在土壤或树上的传感器可以帮助环境保护机构监测农民及其对土地的使用状况。

环境保护监测和应急服务

还记得之前提到过的自主运作的代理人BOB吗？BOB将会生活在一个充斥着气象探头的世界，并通过对重要的气象数据的收集和销售实现营利。这里的例子包括对空气质量和水质的监测并发出警报从而减少污染物水平或让人们留在室内；为应急人员检测危险的化学品或辐射源；监测雷击事件和山林火灾；安装地震和海啸的早期预警和警报系统；除了能够改善应急服务的响应时间和降低这些事件给人类所带来的风险，我们可以使用这些纵向数据提高我们对基础的趋势和模式的理解水平，在某些案例中发现预防性的措施，并提高我们的预测能力从而实现更早期的警报。

卫生保健服务

在卫生保健服务领域，专家们用数字化的技术去管理资产、医疗记录、库存，并为所有的设备和药物处理订单和支付的相关需求。今天，医院里面有不少可以审查这些服务的智能设备，不过很多的设备会与此之间进行通信，也没有考虑到在病人护理的过程中所涉及的隐私保护

的重要性。基于区块链的物联网可以使用新出现的技术将这些服务连接到一起。正在开发的应用程序包括监护和疾病管理（如智能药物，跟踪生物体征和提供反馈的可穿戴设备）以及用于提供质量控制的水平。想象一下，一个人工髋关节或膝盖可以对自身的工作状况进行监测，并将工作状况的数据匿名地传输到生产厂商那里，以用于日后的改善，还可以与病人的医生沟通，如“是时候把我换掉了。”技术人员们在无法采取必要措施确保设备的可靠性和准确性的情况下，就不能使用专用的设备了。新型的智能药物将可以在临床测试的时候对自己进行跟踪，并为自己的有效性和副作用提供相关的证据，而且无须担心有人篡改这些结果。

金融服务和保险

金融机构可以使用智能设备和物联网去追踪他们对实物资产的所有权并实现它们的追踪和溯源。数字货币让大小客户能够更快、更安全地对价值进行存储和传输，也能实现风险评估和管理。进一步思考，如果弱势群体实现他们有限的资产的追踪和分享（就如之前提到过的微电网的例子），那么他们是否就能赚到少量的现金、电力或其他“积分”？物品的主人将可以对贵重的物品、古董、首饰、博物馆展品及任何曾由苏士比拍卖行处理过或由劳合社(Lloyds)承保的物件进行标记。保险公司可以根据物件的位置和所处的环境调整保险费用——如果是在纽约大都会博物馆里的受控环境，则可以降低保险费用；如果是要运输到希腊，那么保险费用就会增加。这个物件将能够告知其他人它是否曾经在一个保险箱里或曾经在某个名人的脖子上。如果这个物件曾经戴在莲莎·露夏恩（好莱坞小天后）的脖子上而非安妮·哈撒韦（美国女影星）的，则它的保险费率将会有所提高。无人驾驶汽车将会有更低的保险费率，而它自己也能在事故现场根据传感器数据直接处理保险索赔事宜。

文档和其它记录的保存

就如我们解释过那样，实物资产可以转换为数字资产。所有与某个特定文件相关的文档可以被数字化并登载到区块链上，这包括专利、所有权、质保条款、检验证书、起源、更换日期、审批等，能够极大地提高数据的可得性和完整性，从而降低所有文书工作、存储和损耗的负担，并改善与该文档工作相关的流程。例如，一个汽车若在最近不能通过一场安全性检查、责任险已经过期、所有者没有交付违章停车罚单或交通违章相关的罚款，或是司机的驾驶证已经被暂停使用了，那么这辆车就无法启动了。货架上的物件会在过期后通知店铺经理。店铺经理们甚至可以对这些物件进行编程，让它们在接近有效期时自动降价促销。

建筑与房产

据估计，在美国的120亿平方英尺的商业地产当中，有65%是闲置的。²²数字化的探头可以通过对实时发现、可用性和支付的支持为这些地产资源创建一个市场。商家们正在进入这个领域，并开发新型的服务模式以在下班时间出租这些空间。在晚上，你的会议室可以变成为街区的少年服务的教室或为本地某个初创企业的办公室。其他应用将会包括安保和访问控制、灯光、加热系统、制冷系统及废弃物和水资源管理。绿色建筑将会在万物账本中运行。想象一下，电梯的使用率和建筑物通行人流量这些数据将对建筑师为公共和私人空间的设计方案有着什么样的参考意义？闲置的住宅空间可以通过万物账本将自己登记到市场中并进行商议，以帮助游客、学生、收容所的管理者及其他人寻找到能够满足需求的空间。这些构思可以应用到所有类型的住宅、宾馆、办公室、工厂、零售/批发及机构的地产。

工厂管理——物件构成的工厂

全球工厂需要一个全球的万物账本，即工业区块链。工厂管理者将会使用智能设备监测生产线、仓库库存、配送、质量和其他需要监察的事项。整个产业可能会采用这个账本的手段极大地提高供应链管理这类

流程的效率。像飞机和铁路机车这样的大型、复杂的机械设备是由几百万个零部件组成的。飞机引擎或动车的每一个零部件都可以安装上传感器，用于在需要故障修复时发送警报。想象一下，一辆火车在开往巴尔的摩至长滩的途中可以在到达长滩的三天前就通知当地的维修人员，让他们准备好一个重要的新零部件。传感器甚至可以发布一个招标启示，并接受为该零部件提出的价格最低、交货期最短的提议，其效率与成本相对于通用电气、Norfolk Southern及其他大型公司的运作有着极大的优势。还有一个更明显的趋势，就是从汽车到灯泡再到创可贴的生产商都在探讨如何能够将智能芯片植入它们的产品或其中的零部件里，并监测、手机和分析使用过程中产生的数据。通过这些数据，它们可以提供自动升级、预测客户需求和提供新的服务，实际上是在从产品提供商转化为持续的、基于软件模式的服务商。

家居管理

感到寂寞吗？你是可以跟你的房子说话的。你自己的房子和各种产品、服务正在进入一个让家居能够实现自动化、远程监测的市场。这些服务比保姆摄像头实现的功能更多，包括了访问控制、温度调节、灯光控制，最终可能是控制你家里所有的物件。虽然“智能家居”的普及速度相对来说还是比较慢的，但如苹果、三星和Google这样的公司正在寻求简化其安装和运作的方法。BCC研究公司发表的报告指出，“美国的家居自动化市场预计会从2014年的69亿美元市值到达2019年的103亿美元市值，这个增长过程将会是稳定的、长期的。”²³

零售商和销售

当你在逛街的时候，你的移动设备会告诉你，“你喜欢的衣服在GAP这家店里有货了”。你进入这家店后，适合你的尺寸的这件衣服已经在等待你了。在你试穿这件衣服后，你扫描一下就可以完成付款了。不过你还有其他事情等着去做，所以这件衣服会被在你回家前自动送到

你家中。除了运作效率和环境监控外，在顾客走路或开车经过商店的时候，零售商可以根据他们的地点、人群分类、已知的兴趣和购买历史自动地为他们提供个性化的产品和服务——前提是这些顾客在区块链上将自己的身份“黑盒子”的特定信息的访问权开放给这些零售商。

经济上的收益

在这个章节中，我们引用了一些关于基于区块链的分布式物联网在多个层面（个人、组织、产业、社会）所能提供的潜在收益。通过点对点网络（而不是人或中心化的中介应用程序）对流程进行重新设计及自动化改造，能够带来很多好处，其中的一些如下：

- 速度（端对端自动化）
- 降低成本（把将近乎无限的数据发送到大型的中心化处理设施时引发的成本；能够去除高成本的中介机构）
- 增加收入、效率和/或生产力（重新使用过剩的资源）
- 提高效率（内置检查清单和其他协议以降低人为错误所带来的影响）
- 提高安全性和正直性（随着信任机制直接被设计为网络架构的一部分，人和人之间的信任并不是必需的）。
- 降低系统失效的风险（消除瓶颈，内置能够抵御风险的特性）。
- 降低能源消耗（网络所需的能源能够被其所提高的效率和降低的损耗、动态定价和反馈机制所抵消）。
- 提高隐私保护水平（中介无法跳过或忽略在区块链中设定的规

则）。

- 提高对基础模式和流程及机会的认识，并通过对“无限的数据”的收集和分析改善这些事项。

- 加强对不同事件的预测能力，不管是负面的（极端天气、地震、每况愈下的健康状况），还是正面的（种植农作物的最佳时间，采购模式等）。

分布式的开放模式意味着物联网可以在公司退出或生产商破产时还能继续由自己运行下去。当系统的设计将互操作性考虑进去后，将可以连接到不同的物联网中，这样能释放出更高的价值。²⁴

这些好处依赖于分布式（去中心化）网络和移除中心（如命令和控制）或其他中介（如清算所或管理应用程序）。当这些新的中介出现后，其他机构将会感到有“绕过”或移除它们的压力。埃里克·詹宁斯认为，“人们会尽可能消除让自己感到不适的事情，这样会导致孤岛效应、集中化和中心化。这些人的短期收益对每一个人都是长期的损失”。他说道，“物联网应该是完全地去中心化的，里面的设备可以自主地运作，直接发现彼此并建立安全的通信，最终可以在机器与机器之间直接向对方支付价值”。²⁵

IBM商业价值研究院进行了一项研究，探讨了基于区块链的物联网所能够带来的五项主要的“颠覆性方向”及其让我们更好地利用实物资产的潜力。²⁶IBM对物联网显然是有商业上的兴趣的，而它对其商业价值的关注也是很有帮助的。

首先，这个研究院注意到这种新的网络会让用户快速地对可用的实物资产（如闲置的存储空间或计算机性能）进行搜索、访问和支付等操作。资产的供应和需求进行彼此的匹配。因为我们可以在线评估风险及信用并及时取回结果，这样我们可以对信用和风险进行重新定价，从而

降低这方面的成本因素。系统和设备的自动运作能够改善运作效率。最后，公司可以实时地通过数字化集成价值的链进行众包、协作及与商业伙伴之间实现优化和协调。

简而言之，你有机会创建一个在概念上更简单、更高效的市场。你可以访问之前无法访问的资产，进行实时定价，并且降低风险。当基础设施就绪后，准入门槛就降低了（如只开发一个应用程序），而且持续的耗费相对来说会更低（如不会再有第三方服务费了）。它极大地降低了传输资金所需的成本，降低了拥有银行账户、获得信用及进行投资的准入门槛。它甚至可以支持微付款的渠道，将按照分钟收费的服务在每一分钟进行付费。

万物账本让“分布式资本主义”成为可能，而不只是现在的重新分配式的资本主义。这还仍然不是为所有人带来的自由，但我们可以根据我们作为个人、公司和社会的价值观去塑造这些市场并将这些价值观编码到区块链中，如使用可再生能源的激励机制、首先使用来自我们邻居的资源、遵守价格上的承诺并保护隐私等价值观。简而言之，随着我们分享的越多，在物联网之上的万物账本就推动了物质世界，使得物质世界更人性化。就如IBM所说的，“在宏观经济的层面，我们都是物联网所创造的未来的赢家，虽然不同的产业将会感受到不同的混合效应”。²⁷麦肯锡全球研究所指出物联网的经济价值一直被低估了；在2025年所有的物联网应用的经济价值（包括消费者盈余）可以达到11.1万亿规模。²⁸这能够在我们当前的全球GDP（当前是超过100万亿）之上增加10%的规模。这具有很重要的意义。

《数字经济》中创造了一个名为“网络化智能”的术语，指的是网络的智能程度要超出网络中最聪明的节点。就如我们解释过的那样，第一代的互联网在某种程度上降低了交易成本。通过很多创新性的商业模式，我们有了更快的供应链、市场营销的新方式及大规模的点对点协作（如Linux和Wikipedia）。区块链技术将会加速这个过程。物联网正在

稳步向前，而这些潮流将会加速。

未来: 从Uber到Suber

在这章里面我们已经涵盖了很多基础的内容。现在我们可以将创新的路线放到一个场景中。

考虑一下像Uber和Lyft这样的服务聚合者。Uber是一个基于手机应用程序（APP）的车辆分享网络，那些愿意搭载其他人的司机将能收取到一定费用。若要使用Uber，你需要下载Uber的应用程序，创建一个账号，并将你的信用卡信息提供给Uber。当你使用这个应用程序发出打车的请求时，它会让你选择需要的车辆类型并在地图上标记你的位置。这个应用程序会向顾客随时通知可用的车辆资源及潜在司机的位置。在车程结束后，Uber会自动从你信用卡中扣款。如果你不想支付默认的小费数额，你需要在Uber网站的账单设置中进行更改。²⁹Uber应用程序背后的开发和运营工作是由Uber有限公司负责的，它会从每一段车程所支付的费用中收取一定的分成。

这听上去是不错的，特别是在出租车资源较为短缺的城市里。不过Uber的服务包含着一系列的问题和危险信号。它已经出现过司机账户被入侵的例子了，另外车程会出现突然的高价，而乘客甚至曾经面对过司机鲁莽驾驶及被其性骚扰或袭击的事情。³⁰另外，Uber也在追踪用户的每一项操作，并将部分信息释放给交通部门以进行交通状况的研究。除了这些以外，司机们创造了相当多的价值，但他们只能得到其中的一部分。

现在，让我们想象一下如果在区块链上的一个分布式应用程序上，Uber这样的模式会带来什么样的用户体验呢？迈克·赫恩是Google的前雇员，他从Google辞职并全职进行比特币的开发，并在2013年的图灵节

上发布了一个基于比特币技术的另类实现方案。³¹迈克·赫恩将这个网络称为“TradeNet”（交易网），并描述了在比特币的帮助下这个系统是如何让人们可以开始依赖无人驾驶汽车的。

它的工作方式如下。大部分人并不拥有汽车，但会与其他人共享汽车。在芝加哥，梅利莎通过SUber（可以看成是基于区块链的超级Uber）。这些可以租用的车辆开始自动地张贴广告，梅利莎的节点对其进行评分并根据她所选择的条件将结果展示给他。梅利莎还将她愿意为最快的路径支付的费用考虑进去了（如更高价的收费车道）。

同时，约翰是一个SUber车辆的持有者（这与大多数用户不一样），它的无人驾驶汽车正在将他送达工作单位，它识别出各种泊车的选项（公共和私有的空间），选择好一个停车位置后就通过自主运作的泊车市场将这个位置保留下来并进行支付。因为约翰预先定义参数总是包括离目的地步行距离10分钟的最低价位置，他通常会遵循他的车辆的第一个决定。底层的泊车数据库同时也包含了与特定泊车规则相关的信息，如特定的街道、特定的日期、每天中的不同时间、泊车位置是有遮盖的还是露天的，以及位置的所有者是否设置了一个最低价等。这些都运行在一个分布式的点对点平台上，将多个应用程序连接起来，因此其中没有中心化的公司在充当订单的中介或参与手续费的分享。这不会存在波动极大的定价机制及意外的费用。

这个模式的显著之处并非无人驾驶汽车本身，因为无人驾驶汽车将会是很平凡的东西了，可能比想象中所需的普及时间还更短。其显著之处在于，这些车辆将会是完全地自主运作的代理人，可以赚取自己的经费，为自己的燃料和维修任务付款，获得自己的汽车保险，在出现碰撞时自己商量责任的划分，并在没有人类控制的情况下运作（“开车”）——除了在它们需要与某些组织或人在法庭上处理法律问题时。

SUber的管理员应该将车辆的协议编程到区块链上，以遵守所有的

交通规则、选择最直接、最快或最廉价的路径，并遵守其关于所接受价格的承诺，这些都是运作所需的条件。司机们在首次往SUber系统上登记信息时，可以要求车辆注册必要的文档，这包括安全检查和保险相关的文档，而系统将会永久性地保留这些记录，以确保所需的复验、保险和执照更新等事项能够顺利进行。传感器可以监测车辆总体的“健康状况”，在合适的维修店预约时间，并预先订购任何必需的零件。由于车辆是无人驾驶的，因此乘客并不会碰到讽刺、态度倾向、性别歧视、种族主义或其它形式的人类特有的歧视或堕落的问题。这些都是在后台进行的，在物件之间进行的，是由一个自主运作的应用程序所驱动的。司机们这样就能创建一个基于区块链的合作社（就如前面章节讨论过的那样），他们在这个模式中能够获得几乎是所创造财富的全部份额。至于像梅利莎和约翰这样的用户，只会得到便利，而没有各种麻烦事。这还有什么不好的地方吗？

虽然互联网降低了搜索和协调的成本，但区块链上的数字货币（如比特币）才将让我们能够降低商议、签订合约、管理和执行这些合约的成本。我们将可以通过商议获得最佳的条约并从任何接受比特币支付的实体（包括一辆无人驾驶的出租车）获得所承诺的货物或服务。Uber这类的业务将怎么与之竞争呢？

不过这个场景并不是到这里就结束了。植入到城市基础设施的智能设备将会改善交通运行状况（基于交通流考虑不同的车道方向、不同的定价和自动化的交通信号管理），从而进一步地降低能源的耗费和各种成本。区块链可以实现车辆（不管是有人驾驶还是无人驾驶的）及基础设施的安全控制，如接近警报和自动刹车，以及防盗和禁止无资格的或酒醉的司机开车。还有，城市将会使用传感器去辅助交通基础设施的管理，这包括基础设施和车队的资产管理、监控铁道和人行道的状况、生成维修计划和预算并在需要的时候派遣维修队。

这些系统的结合是真正强大的地方，如智能汽车在智能的基础设施

里运作。共享的车辆依然会有对人类司机的需求，但自主运作的车辆将会通过内置的导航和安全系统在城市的街道上通行，并会经常与智能的基础设施互动，从而寻找和支付加速车道或停车位，或寻找一条首选的路径。这就如上面的商业地产的例子那样，资源经常处于闲置状态，得不到充分利用，而无人驾驶汽车的可得性、可负担性及可靠性将会极大地降低私家车的保有量。

技术公司或汽车公司并不会是搭建这套系统的主导者。这些系统在理论上可以被单一的城市运输管理当局开发、控制、运作和管理，但事实上不太可能用这个方案。SUber将更可能作为一个开放、共享的交通平台的形式实现其进化和创新，而这个平台之上本地企业、社区组织、政府、营利组织（若通过无人驾驶的车队所赚取的收入）、共享的合作社（如一个邻里组织投资了10台车辆，并使用SUber的应用程序进行保留了分享）、公共服务（如在一条需求较高的路径上维护和运营一辆火车或快车）或社会性企业（如非营利组织可以投资SUber的积分，这样它们的客户就可以在需要交通工具的时候使用这些积分了）都可以开发和引入各种应用程序。

这些事情可能会先在具有以下特征的辖区出现：已经有各种独立的交通方式的（如铁路、公路、自行车、步行）辖区，有着明显交通问题的辖区（如交通堵塞），以及有着遵守交通规则的良好传统的人群所居住的辖区。这或许它可能会在“greenfield”的城市开发中，与技术公司和汽车公司合作以寻找它们应用项目的试验台。如果其他的道路使用者不能被隔离开来（在不同的交通通道上）、不能被预测（如路上的动物）或不能被控制（如分心的行人），那么涉及无人驾驶汽车的场景可能就会没那么成功（甚至是很危险的）。

Suber的场景是越来越可行。这样的应用程序将有可能在未来几年出现并在长期逐步地解决我们的交通需求。今天，本地的出租车和豪华轿车组织已经在多个城市对抗Uber，而各个城市政府正在努力地平衡

顾客对可负担出行选项的要求与公共安全和出租车执照管理的冲突，即使Uber这样的新模式看上去已经是无可避免了。为什么不关注一下交通部门的发展方向如何并设计最能满足城市需要的解决方案呢？这就如在我们假设的SUber场景中芝加哥所做的事情一样。

用智能物件的世界改变你的未来

在这一章中，我们看到了在几乎是我们生活中的每一个角落都存在的难以置信的机会，这包括（或许特别是）在未被数字化革命的第一波影响过的领域。同时，这些机会给现有的商业及营商方式带来了挑战。

关键问题

作为一个管理者，你为什么应该同时做等号两边的事情——实现新机会的同时将所带来的威胁降到最低。无论你是在公共、私营或社会部门的管理者，你有一些未被充分利用的实物资产可以用于实现更多的价值吗？你意识到为物联网开发产品和技术所带来的最大效率与机会吗？进入这个经济体的新竞争者会通过发明新的“基于app的商业模式”抢走你的客户并降低你的收入吗，而这些商业模式本来就应该先由你去部署的？

新价值

你的实物资产是什么？你如何能够将其增强并为你的组织或社区带来更多的价值？你建立了一个自主运作的网络并对其设置了运作参数，若你有一些现实世界的空间、机器、库存或其它资产可以进行标记、监视并赋予活力，你可以将这些资产作为这个网络的一部分以降低成本或增加价值吗？你能嵌入、升级传感器并对其进行编程，从而将其作为大型网络的一部分而实现更多的功能和价值吗？你能从物联网中收集到新

的信息并改善你对未来的计划和分析吗？

新商业模式

基于你能够通过网络收集的这些新功能和数据，有什么新的产品和服务能够在其之上实现？若你的信息和资产对他人是有价值的，那么你能通过它获取收入吗（如出租闲置的高价值设备）？商家对信息的价值进行关注并不是什么新鲜事了（还记得Sabre和美国航空公司吗？），但在目前有一些信息的价值还是被忽略了。

机会

你能将你的网络与其他的连接在一起从而实现更高的价值吗？或许是作为一个点对点供应链或配送和销售渠道的一部分？作为一个产业，会有什么可以共享的流程和功能可以通过区块链进行自动化改造吗？你有在使用建立在开放标准并通过国际协作进行审查的技术来实现这种互操作性吗？

威胁

你当前正在为一个市场提供服务，而新来的竞争者会在这个市场内使用他们的基于物联网的新商业模式去进攻哪方面的业务？例如，如果汽车、个人消费品或定制设备的一次性销售模式不再流行，进化成依赖于你与该设备的持续连接之上的新服务模式，对你和你的客户来说这会产生持续的价值吗？你能用你现有的技能、资源、基础设施和顾客忠诚度去设计新的基于物联网的商业模式，从而作为一个新的颠覆者加入市场吗？

商业案例

这些机会的耗费和好处是什么？对你的机构来说它能在哪个地方发

挥真正的价值？你是在解决一个实际的商业问题或需求还是只是寻求最新的技术？可以与一个牵头的客户共同开发一个概念验证产品吗？

战略规划

根据麦肯锡咨询所说的，“管理层将要处理三种挑战：组织失调、技术互操作性、分析障碍及更高的网络安全风险”³²。我们会在这个列表中加入第四个主要挑战，即内建一个隐私与激励机制计划，包括一开始就引入适当的保护机制。IT和商业运作应该如何适应物联网？你应该将机构的哪个部分及哪些商业领袖考虑进来？

第七章 解决繁荣悖论：区块链的经济包容性

一头猪不是一个存钱罐

尼加拉瓜的太平洋海岸是美洲最美丽的景色之一，在那里翠绿的森林和蓝色的海水交汇在一起，直至无尽的远方。此起彼伏的山峦和令人炫目的海滩，使得那里成了背包客、日光浴者和生态旅游者们等等的首选目的地。但尼加拉瓜也是那个地区最穷和最欠发达的国家之一。60%的人口生活水准在贫困线以下。当地旅游业从业人员以外的人口靠着仅能勉强维持生计的农业和渔业谋生。尼加拉瓜有着美洲第二低的名义国民生产总值，而其整个GDP中有10%源自于汇款，即尼加拉瓜外侨在海外赚得并汇回的钱。19%的尼加拉瓜人拥有一个正式的银行账户，但其中仅有14%的人能够借款，而仅8%的人有正式的储蓄。¹但93%的人已申请有移动电话，通常以预付费的形式入网。²

那就是乔伊丝·金把她的团队带去尼加拉瓜时所面对的现实。乔伊丝·金是恒星币开发基金会（一家区块链技术的非营利组织，别把它和一个名叫Stellar的大型建筑和建设公司混淆起来）的执行董事。一个尼加拉瓜的小微金融运营商曾想要进一步了解恒星币的金融平台的情况。尼加拉瓜那悲催薄弱的银行业把大多数人困留在了无法脱身的贫穷循环之中，也加剧了那些未来企业家们的困境。他们努力创立新的企业，注册土地和其他资产的产权，并解决桑蒂尼斯塔政府在20世纪80年代的大规模土地征收的遗留索赔问题。³恒星币的平台将帮助尼加拉瓜对于金钱的转移、储蓄、投资、借款和放贷。

对于当地致力于小微贷款的专注程度，乔伊丝·金既感触颇深又惊讶。她知道，能够获得贷款对于经济包容性而言是至关重要的，但她也相信储蓄（即可靠安全地存储价值的能力）是几乎所有其他金融服务的一项前提条件。当乔伊丝·金问到储蓄时，她被告知“哦，储蓄在这里不是个问题。人们有猪”。⁴

在很多农业经济体中，家畜构成了农民的绝大部分资产净值，因为金融服务并未广泛可及，个人也对财产和土地产权没有扎实的权利。这在尼加拉瓜意味着人们拥有猪，而且有很多。乔伊丝·金起初很惊讶，但很快看到了这其中久经考验的逻辑。“你从一个会议中出来，环顾四周然后发现到处是猪。”⁵家畜长期以来一直是一种被公认的且相对有用的储蓄形式。对于那些被排除在数字经济以外的人们来说，动物几乎就是你能拥有的最具流动性的资产了，尤其是如果它们能够产奶以及能提供猪仔、鸡蛋、羊羔、牛犊以及有时候是奶酪这样的“分红”。

富裕是个相对概念。在肯尼亚，马萨伊部落中拥有400~500只山羊的人就被视为富裕了，但他们的生活可能是粗糙、野蛮和短寿的。基于家畜的财富是“高度本地化的，以至于你实际上无法与任何其他人进行交易，除非对方就在你面前”，乔伊丝·金这么说道。“你面临着巨大风险，诸如动物逃跑、生病或一些可能会让你所有的积蓄化为乌有的疫情时有发生”⁶。

信贷是一个甚至比储蓄更麻烦的难题。金认识了个当地渔民，也是一个合作组织的成员，他解释说：没有哪个渔民能借到足够的贷款来给船只配上成套完整的帆装。按乔伊丝·金的说法，“人们是这么组成捕鱼队的：一个人拿到贷款买网，另一个人拿到贷款买鱼饵，另一个人拿到贷款买船，再一个人拿到贷款买马达，然后他们就一起出发，组成了一个捕鱼船员的团队”。没有谁能够独自筹资让他或她的事业起航，因为贷款是如此紧张。前述那个模式有用，但它牵扯到和渔民数量一样多的中间人。

尼加拉瓜渔民和农民们一生的融资困境就是大部分缺乏银行服务的人们故事，今天在世界上大约有20亿成年人属于这种人。⁷他们所缺乏的是不会得疯牛病或老死的价值储存方式，或是能够延伸至本村之外的支付手段，而我们将这些条件视之为理所当然。

金融包容性是经济包容性的一个前提。其影响延伸至金融以外。乔伊丝·金说：“我并不认为融资渠道和金融包容性是终极目的。这只是一条通向更好教育、更好医疗服务和妇女平权和经济发展的道路，我们必需走过这条道路。”⁸简而言之，金融包容性是一项根本性权利。

本章考察了移动通信和金融服务提供商和其他企业使用区块链激发出处于金字塔底部的经济潜能的机会。我们讨论的是百万计的新增用户、企业和资产持有人，他们准备就绪随时待发。记住：区块链交易可以是十分微小的，是一个便士的几分之一，且几乎不需要成本即可完成。任何拥有最小资产的人，比如在刺绣或音乐方面的天赋、多余的水桶、生蛋的鸡和能记录数据、音频和图像的手机，都可能交换价值。新的平台也消除了访问节点的障碍。如果你能够用移动设备访问互联网，则你就可以存取资产，既无须填写任何表格也几乎不需要什么识字水平。这是些看上去很小、但具有不可思议的重要性的突破。如果我们做得对，区块链技术能够释放出史上最大的尚未被开发利用的人力资本池，把数十亿计已投身于蓬勃发展的事业之中的企业家们带入到全球经济之中。

新的繁荣悖论

有史以来第一次，全球经济虽然增长但却几乎无人受益。一方面，数字时代正在给创新和经济发展带来无穷无尽的可能性。公司的利润犹如气球一样膨胀。另一方面，繁荣程度却停下了脚步。发达国家的生活标准甚至下降了。在现代历史上，经济水平位于统计学的第51百分位的

个人和家庭的数量一直有所提升。尽管出现过萧条和动乱，对这些人及社会整体来说，繁荣的程度还是在稳定提升的。但现在已经不是这个情况了。即使在发达国家，生活标准也出现了下降。OECD（经济合作与发展组织）国家的工资中位数增长正在停滞。此外，根据国际劳工组织，世界上大部分地区的年轻人失业率维持在20%左右。世界劳工组织曾报道：“年轻人的失业率几乎是成年人的三倍”。⁹在大部分发展中国家，这些数字则又要高得多。这些失业对所有社会都是腐蚀性的，无论社会的发展程度如何。大部分公民想要对他们的社区做出贡献。任何曾经丧失过工作的人都知道失业会如何侵蚀任何的自尊和幸福。拥有权力和财富的人跑在了前面，而没有权力和财富的人则落在了后面。

这种新的繁荣悖论——不要把它和吉尔伯特·莫里斯等经济学家们所创造的代际间“繁荣悖论”相混淆起来——已经让西方世界的所有政策制定者们困惑了。2014年的最畅销商业书籍，托马斯·皮凯蒂的《21世纪资本论》是一本学术界的代表大作，它解释了为什么不平等在加速产生，并且只要资本回报超出长期经济发展，这种趋势很可能会持续下去。富人更富，是因为他们的钱能够产生比工作收入更多的钱。因此，新的百万富翁和亿万富翁正在不断产生。但对于如何阻止社会不平等加剧，他的解决方案是对拥有世界上大部分财富的人们进行征税，这个方案并不那么鼓舞人心，因为我们曾经听到过。¹⁰的确，只要资本主义仍是生产的根本模式，关于如何分享成果的争论就从未实质性超越于财富再分配，这种再分配通常是通过富人征税和对穷人提供公共服务的方式。我们当前经济模式的鼓吹者们言必称发展中国家数以亿计的已从悲苦贫困中脱离了出来的人口（大部分在亚洲），但却经常性地忽视了富人们所被赋予的不均等的利益以及超级富豪与本国其余人之间正在扩大的鸿沟。今天，全世界1%的人口拥有全世界一半的财富，而有35亿人的每天收入低于两美元。

现状的维护者们迅速指出：世界上大部分超级富豪都是通过开立公司而发财致富的，而不是通过继承。但是在一些成功案例的背后，却是

一些十分复杂的统计。新企业的开办率正在下降。在美国，历史短于一年的公司占比在1978到2011年间下降了接近一半，从15%下降到了8%。¹¹千禧一代经常被描绘为具有企业家精神的风险承担者，他们却几乎没做什么来反抗这种趋势，相反却可能在促进这种趋势。美联储近期的一项分析数据发现，户主年龄低于30岁的美国家庭中只有3.6%的家庭才在私人公司中持有权益，低于1989年的10.6%。¹²

在发展中国家，数字革命几乎没能帮助企业扫清充满着种种障碍的道路。在OECD国家需要花费仅3.4%的人均收入来开办企业，在拉美则需要花费31.4%，而在撒哈拉沙漠以南的非洲则令人震惊得高达56.2%。在巴西，一个企业家要等几乎103天才能注册成立公司，相比之下在美国只要4天，而在新西兰只要半天。¹³出于对政府的膨胀和低效的反感，发展中国家的很多潜在企业家改为选择在所谓的非正式经济中经营业务。赫尔南多·德索托说过，“在西方世界有很多事物你觉得是理所当然的。例如财产记录是遵循规矩的。而在南半球，企业家宁可政府不知道他们的存在。我们需要把正式身份变成一个有利可图的东西”。目前，躲藏在阴影中能够使这些企业家避开那些雁过拔毛的官员，但这也深远地限制了他们发展壮大事业的能力，限制了权利，也使得原本可以可被更高效利用起来的金钱成了“死的资本”。¹⁴此外，即使对于那些在公开环境下经营公司的人们，很多国家的法律并不提供有限责任。如果你的公司倒闭，你将掉进入个人需承担所有债务的坑里。在有些国家，如果你的一份商业支票被退回，你会直接被抓进监狱。“拘票-立刻坐牢，不会经过‘由此去’”^[1]，也不会经由任何其他机构采取正当的审判程序。¹⁵

好吧，那么这个世界总是有得有失。现在饿死、因疟疾或暴力冲突致死的人减少了。相比起1990年，现在生活在极端贫困中的人口也减少了。¹⁶某些新兴经济体从制造业外包和经济政策自由化之中受益了，中国是最主要的例子，而大部分发达国家的公民平均收入也增加了。总而

言之，人们的日子比过去更好，对吗？所以富人只不过碰巧拥有更多得多的财产那又如何呢？难道他们不该享有努力挣来的钱吗？这到底有什么问题？

皮凯蒂指向了资本主义。但是资本主义作为组织经济活动的一个体系，并不是问题本身。事实上资本主义对于那些知道如何利用它的人们而言，是一条创造财富和繁荣的伟大道路。问题在于大部分人们从未成功看到这个体系的好处，因为现代金融这种（把简单问题复杂化的鲁布·戈德堡机械，如同用高射炮打蚊子），使得很多人无法接触到这个体系。

金融和经济的排斥性就是问题所在。OECD总人口中的15%与任何金融机构都没有发生过业务关系，而墨西哥等国则有73%的人未获得银行服务。在美国，15岁以上人口中有15%没有获得银行服务，这等于3700万美国人。¹⁷

金融不平等是一种会快速演变成社会危机的经济状态。¹⁸2014年，在世界经济论坛（它是一个多股东的组织，其成员包括世界上最大的公司和最有权力的政府）上曾主张：愈发严重的不平等已造成了全球最大（没有之一）的风险，它已经超过了全球气候变暖、战争、疾病和其他灾难。¹⁹区块链可能是解决方案。通过降低金融包容性的壁垒以及催生出企业家精神的新型模式，市场的兴奋剂可能被拿来激活数百万缺乏银行服务的人的梦想和想法。

繁荣的遭罪：无用的作为

几个世纪以来银行一直依赖于网络效应。连续不断的客户、分支网点、产品、存款和提款增加了银行网络的价值。但是建立这些网络是有成本的。具体来说，获取那些能转化成利润的客户的成本一直在上升。如果预期赚到的钱不能覆盖维持成本，银行则没有兴趣再继续维持。因

此，银行几乎没有经济激励去赢得那些处于金字塔底部的客户。根据泰勒·文克莱沃斯所说，银行并不服务世界上大多数人，目前也没计划要服务他们。但是新技术可能会消除那个步骤。他说道：“许多非洲国家用蜂窝式无线通信技术跨越了陆路电线通信的基础设施。他们跳过了那个阶段。区块链将在支付网络缺乏或极端薄弱的地区拥有最大的影响力。”²⁰区块链将推动起许多新生的计划，诸如肯尼亚的移动金融服务提供商M-Pesa（由Safari电信公司拥有）以及全球各地的小微信贷机构，通过把它们变得公开化、全球化且迅捷化，让它们的发展速度挂上高速挡。

银行是最常见的金融机构，所以我们在这里用它来举例。你是怎样开一个银行账户的？如果今天你住在发展中国家，你可能必需亲自跑去银行分支网点。在尼加拉瓜，每十万人只有7家银行分支网点，相比之下美国则是每十万人有34家。和非洲很多国家相比，尼加拉瓜的银行似乎还挺充足，因为前者每十万人只有不到2家银行分支网点。²¹因此你很可能不得不跑大老远才能找到一家银行。你也必需拿着政府颁发的身份证件，但如果你之前还没有，那获得这种证件会非常困难。

在发达国家，比如美国，你需要满足特定条件。虽然这些条件在各银行间和各州间都不同，你通常需要存入款项并且使账户的最低余额保持在100到500美元之间。你也需要证明你自己的身份。在美国开业的银行必需遵守严格的“了解你的客户”、“反洗钱”和“反恐怖主义融资”条例。²²因此它们在给申请人开立账户之前，必需对申请人做更全面的背景调查。最终，银行对你的品质特征进行评估的兴趣还不如它遵守监管机关规定的兴趣来得大。这意味着一份载明有各项要求的明细清单。首先你得有一张社保卡。你没有？那就通常足以把你拒之门外了。那带照片的身份证明，比如驾驶证或护照呢？你还没有？你不是来开银行账户的吧。那假定你既有社保卡又有带照片的身份证明。银行为了安全起见，要求提供近期的公用事业账单作为永久居住地的证明或要求提供先

前银行账户的某些证明。如果你正好是新来乍到来到此地的，或和家里人住在一起，或来自于世界上一个完全没有银行的地区，那你就很可能无法通过这其中的某些检验。银行并不想让你成为客户，除非银行能基于各份准备妥当的证明文件来确认你的身份。银行并无兴趣把你视为一个完整健全的人来深入了解。它只是有兴趣把你当成一长串需要打钩的框框来了解。之前曾经出现过一些为移民和穷人简化这个过程的尝试，像纽约的计划是让人们使用城市ID卡，但最终都失败了。²³

繁荣的护照：有用的作为

对于无银行服务的人们而言，幸运的是区块链技术正在带来一种新型的金融身份。它并不依赖于一个人与银行的关系，而是植根于一个人自己的声誉之中。在这种新的范式之中，“已获有银行服务”并非再是个先决条件。个人能够创建一个持久性的数字身份证以及可核实的声誉，公开明示地在很多关系和交易中开展活动，而不再需要通过那些传统的身份验证。区块链对这种数字身份赋予了信任和获取金融服务的途径。能超大规模地做成这事是史无前例的。ConsenSys的约瑟夫·卢宾说：“我们声誉，但它没那么容易使用，因为社会和经济系统早已建立在那儿了。它的大部分都是缥缈且短暂的。即使在最好的情况下，它是也碎片化的，你因此必需为每项需要提供声誉证明的事业而重新出示一次那些肤浅的证明文件。而在最差的情况下，有数十亿人则根本无法向直系社交圈以外的任何人出示自己的声誉。”²⁴声誉也可能表现为一只猪或一头牛。但是通过底层的基础建设，人们能够建立起非碎片化的或虽然虚拟但却普世且标准化的数字身份，能够强有力地证明它们自己的各个方面以及它们之间的往来互动。人们能够细节性地共享这些数字身份，即仅仅共享关于他们身份中非常特定具体的信息，以促进产生更多的可能带来个人财富增长和富裕的交往互动。戴维·伯奇是一个密码学家和区块链理论家，他总结说：“身份就是一种新的货币。”²⁵

考虑一下这种可能性：世界上那些无银行账户者们当与小微放贷机构发生业务互动时，就能够给他们自己建立声誉档案。潜在的卖家或放贷人能够不再依赖于某些信用评分，而是在区块链上直接追踪到无银行账户者们对小额贷款的使用和偿还情况，这种追踪在以前还是根本不可能做到的。“一旦某个过去无银行账户的人偿还了一笔小额贷款，他们就开始变得渐渐能获得更多更大额的贷款来开创他们的事业了”，²⁶鲁宾说道。一旦重复这种行为，就可以增加借款人的声誉分数。与一个全球性且无摩擦的支付平台结合在一起后，个人和小企业主可以做到以前做不到的事：向一个远在天边的卖家支付货款或服务费，以此提升在全球经济中的前景。乔伊丝·金曾开玩笑说：“我们来基于家务历史记录做出个针对妇女的信用评分体系怎么样？”²⁷经济和金融的断层线经常就是沿着性别分界线而划的，这使得区块链这一技术成为了世界上那些被剥夺了权利的妇女的恩赐。在提及全球各地的穷人时，赫尔南多·德·索托说道：“并非他们不想融入全球经济中来，而是能帮助他们融入经济体系中的标准和信息尚未到位。区块链非常棒，因为它为我们提供了一个能把所有人汇聚起来的公共平台。”²⁸

这种持久性的声誉对全球的企业家才能而言可能意味着什么？如果你有一个可靠、独特且健康的身份，并且你如果被视为是可信任的，那么对方将更乐意为你提供那些获取价值的途径。这并非是财富再分配，而是更广范围的机会分配。“个人黑盒子”的首席执行官哈洛克·库林说：“即将发生的最大的再分配并非是财富的再分配，而是价值的再分配。财富是你拥有的金钱。价值则是你所参与的对象。”²⁹区块链给每个人分配了独一无二且可核实的基于声誉的身份，使得他们能够平等地参与到经济中去。这样的平等性所带来的影响是深远的。鲁宾想象中的未来，在那里“无论人们有没有获得银行服务，都将越来越从贫穷中被解放出来，因为小额放贷服务使得全球投资者们构建起海量小额贷款的多样化信贷资产，使用和偿还这些贷款的完整细节都能在区块链上被追踪到，只要使用比如Balanc3（ConsenSys所投资的一家公司）的三重式记

账系统。”³⁰在这个新的未来之中，当人们偿还小额贷款时，他们在这个过程中能逐渐获得更多、额度更高的贷款来开创他们的事业。

通往繁荣的路线图

金融身份代表着广大金融和经济性机会的开端，而这些机会是世界上超过20亿人曾经无法企及的。区块链技术让各行各业的人们规划出他们的兴盛。想象一下：一个人的个人财富，让很多人所用，最终让几十亿人所用。

充裕的工具

参与到经济活动中来的最基本要求是工具，比如手机和某些互联网接入设备，它们是帮助人们能够与不同价值系统进行互动的入口。Andreessen Horowitz的管理合伙人以及斯坦福大学的讲师巴拉吉·斯里尼瓦桑博士说：“如果你能用手机连上互联网，瞬间你就能接触到所有其他这些东西了。你能访问一个银行或至少是获得访问银行的途径。”³¹区块链技术创造了一整套之前无法想象的新商业模式，赋予了个人成为经济主体的权力。

持久的身份

你能够使用并转移身份进入到不同的网络之中，以此在金融交易中树立声誉或融入不同的社交关系网之中。突然间，猪无须再作为家庭的储蓄罐。用以储存价值以及与其他人交易的新支付渠道和手段，将开辟出一片新天地。实际上，这种降低金融包容性的门槛，将使得发展中国家和发达国家的企业家们创办企业要比以往更容易得多。这其中包括了方方面面，从开通支付渠道到提供可靠价值储存方式乃至到使用区块链软件管理财务报表。

民主化的企业家才能

在合适的条件下，企业家是社会经济增长的引擎。他们为市场带来全新的思考，并注入那些能使得市场经济兴旺发达的创造性颠覆力量。区块链技术赋予了世界各地的个人和小企业与大型组织机构所相同的很多能力。基于区块链的账本和智能合约降低了创办公司的门槛，加快了设立公司的步伐，砍掉了繁文缛节，这些在发展中国家尤其如此，因为在那里设立公司要花三倍的时间且五倍的金钱成本。

区块链能够对建立企业的三个方面进行自动化、精简化以及重大改进：设立、筹资和销售。设立成本将大幅度下降，因为区块链是一种被信任且被广泛知晓的设立公司的方式。你能轻易地看到所有权和维护记录，这些尤其在法治缺失的地区将非常有用。为一个公司筹集资金也将变得更容易，因为你能在全球范围内获得股权式和债权式的资本，而且如果你使用一种通用的计价货币如比特币，那么你就无须担心汇率和兑换问题。销售将成为一种能够卖至任何一个有上网装备的人的功能活动。买家根本无须信用卡、当地货币或银行账户。

通过安全且不可篡改的账本，企业家将能够注册他们的企业和公司资产的产权；管理存货、应付款和应收账款；以及通过三重式记账软件和其他区块链应用来杠杆运作其他财务指标。例如，三重式记账减少了对审计师、税务律师和其他服务供应商的需求，这些供应商对小企业而言是个巨大负担。³²监管者也许会对选择加入三重式记账计划的小企业放松监管。那对本质问题的意义更加重大，而减少了浪费的时间。随着公司的成长，对公司行动和文件进行协调一致将变得不那么复杂。通过智能合约，一个企业家能够自动化处理公司运营的很多方面：订单、薪资发放、债务利息和实时财务审计。个体企业家的两种新模式将受到欢迎。

过剩物资的打表计量

从中心化的共享经济到分布式度量经济，个人将能够基于网络中的其他参与者们的声誉分数，向他们出借备用睡床、手推车、牛乃至其他有形无形的资产。区块链为之前不可能实现的收入来源带来了可行性，比如打表计量无线信号、屋顶安装太阳能电池板所发的电力、Netflix的订阅、你手机的隐藏算力和其他家用电器，而实现这一切都依靠小微支付和智能合约。区块链成为个人以非传统方式创造价值和赚取收入的新的公用事业。

被小额变现的数据

那些在家里工作的父母以及不知疲倦地照看小孩和老人的各类家庭看护人员，能够至少把他们的辛勤劳动进行货币化，并且他们一天中每个小时所产生的价值将能被得到承认。这并非仅仅是发达国家才享有的机会。大公司们正在寻找向南半球的人们进行市场推广的途径，但经常缺乏合适的数据来做商业决策。当一个年轻的企业家正在推出他的新的区块链IPO时，承包并许可使用数据对他而言可能是个能带来新增收入的巨大机会。今天，像Facebook和谷歌这样的大型数字行业综合性企业正在收获着关于几十亿人的千万兆字节量级的数据。我们订立了一个浮士德式的交易，在这个交易中我们用数据换取很酷的服务，但我们在此过程中丧失了隐私和数据完整性。区块链把顾客们变成了“产销者”。耐克公司可能想知道你早餐吃什么、隔多久跑以一次步以及是否考虑买新的训练装备。为什么不签订合同用那些数据来换取耐克的积分或金钱呢？让我们再进一步，保险公司正在搜索最好的数据用于精算。你自己的数据，如运动量、你是否抽烟、你的食物选择等，对它们而言都很有价值。你可以订立一个许可协议，据此每次它们使用你的数据来做精算以及为某一产品定价时，你就获得一小笔付款。[33](#)

分布式所有权和投资

我们正在前进到人类历史的一个新时期，很多人能够通过分布式账

本技术成为财富的主人。一旦能够接触到世界金融市场和全球投资机会，从传统投资到参加大规模合作创业、小微贷款计划、区块链IPO和基于声誉的小微贷款，这就开启了通向资本之路。众筹已经开始改变金融业的外表。在2012年，非区块链的众筹活动在全球范围内募集了27亿美元，比上一年增长了80%。而有了点对点的众包式的区块链融资后，这些数字准备再翻上几倍。个人能够通过众筹计划来认缴微小的金额。想象一个众筹计划涉及了几百万人，每个人认缴一美元。把它称为分布式的所有权。你觉得这没意义？Augur，作为预测市场的平台，从全球成千上万人那里募集了几百万美元，每个人的认缴增额幅度都很小。可能性的范围是巨大的。区块链IPO不仅仅能够改进募集资金的效果和效率、降低发行者的成本，还能够具有广泛的包容性，让那些曾经无法想象的新兴投资者们加入进来。到目前，改变收入和财富不平等的方案范围尚未超出对富人加税这一方面，最极端的版本则是直接国家征收。让我们想象区块链将如何创造机会来更平等地分享社会创造的财富，而不是财富的再分配和征收。

汇款：安娜丽·多明戈的故事

安娜丽·多明戈³⁴已作为保姆和家务工工作了25年。她是生活在多伦多的20万菲律宾人中的一个³⁵，她的故事十分典型：她年轻时离开菲律宾前往加拿大定居，此时毫无积蓄、没受过任何教育并且对接纳她的国家基本上一无所知。安娜丽工作非常努力，为自己和家庭开辟出一条谋生之路。十年前，她用自己的积蓄付了一幢房子的订金，这是个惊人的壮举，因为她在此前三百个月里一直孝顺地把钱汇给菲律宾的家人。安娜丽向家里汇了如此多的钱，以至于她70岁的妈妈能够在马尼拉买了自己的房子。

安娜丽亲切地同意让我们在发薪日去找她，记录下她的经历。那个星期五下午，安娜丽拿到了她雇主手签的支票，并递给了银行。这花了15分钟，如果算上在银行出纳那里的排队时间，则花了20分钟。当她把

支票存进银行后，她提取了200美元。冰冷发硬的纸钞在手，安娜丽走了一个街区去搭乘公交车。她没有搭回家的公共汽车，而是朝反方向乘了两英里，然后在一个只能被称之为恶邻环绕的地方下了车。她又走了四个街区，最后终于到了她能把钱汇出去的所谓“金融机构”：位于多伦多圣詹姆斯镇某住宅街区尽头的一个iRemit（自助汇款）柜台，该镇是加拿大最穷且危险程度最恶名远扬的地区之一。由于大部分用iRemit服务的人都没银行账户，iRemit已开始提供其他金融服务，例如支票取现。安娜丽像之前数百次所做的那样填写了纸质表格，然后把辛苦挣来的钱交进去。对于一次200美元的汇款，安娜丽付了10美元的固定费用。在收款方那一头，她70岁的母亲要承担差不多麻烦（也几乎一样荒谬）的流程才能收到钱。当然她必需等上三到四天才能去银行，因为这是处理付款所需的平均时间。安娜丽步行回到公交车站，上了车、地铁以及又一辆公交车，最终在一小时后到了家。

汇钱的成本10美元等于总金额的5%。此外，通常还有汇率买卖价差大约1%~2%。最终大约7%，这相较于国际平均水准7.68%而言是少许打了个折。³⁶虽然她们都获得了“银行服务”，但仍旧不得不跑一遍流程，这个事实使得整个可笑的例行程序愈加令人发指。固定成本并未包含入全部成本。例如按工资标准来计算，安娜丽浪费了两小时做这事的时间价值又等于40美元。此外，她不得不提早下班，因为她觉得天黑时去那个地方不安全。而对于她的母亲而言，作为一个生活在马尼拉的古稀之年的老人，去跑一趟取钱对她身体的生理负担同样巨大。安娜丽因做出这个交易而失去的10美元的购买力，对安娜丽而言当然是很重大的，但对她母亲而言则更重大得多。在加拿大10美元是吃顿饭的花费和公交车票花费，而在马尼拉则可以买到一周的食物。在她的一生中，安娜丽为了汇款回家，已经向西联汇款等中介机构付了成千上万美元。每个月的费用最终贡献出了全球每年汇款费用总计高达380亿美元的大蜜罐。³⁷

居住在远方的人们向祖国的资金汇回，联系着全世界散居各处的侨

民们。侨民是分布在全球的社区，其组成者是离开祖先故土散居各处、但共享着相同文化且对故土具有强烈认同感的人们。

今天许多侨民的功能之一就是处理并帮助解决共通性且全球性的问题。汇款是发展中国家最大的资本流动项目之一，可能对某些世界上最脆弱的人民的生活质量具有巨大的正面影响。在某些国家，汇款是当地经济中占比极大且生死攸关的一个组成部分。例如在海地，汇款占当地GDP高达20%。菲律宾每年收到240亿美元汇款，是其GDP的10%。³⁸根据国际货币基金组织的调查，收款人通常把汇款用于购买和支付必需品，如食物、衣服、药物和住处，这意味着汇款“被用以维持原本无法企及的更高消费水准，以此帮助大量人口摆脱贫困”。³⁹流入发展中国家的汇款估计达到外国援助流入的三到四倍。⁴⁰汇款对于发展中国家穷人的正面影响很容易被理解，但尽管这是一项规模极为巨大的资本注入，其汇款成本却仍然高得惊人。在各国之间某些最贵的通道，汇款费用可能超过20%。⁴¹

加拿大是世界上最大的资金净汇出国之一。安大略省无论是按人口还是按经济规模而言都是加拿大最大的省，在那里有三百六十万人被视为是外国出生者，每年数十亿美元以汇款方式流出该省。⁴²安娜丽的故事之所以引人注目，是因为这在加拿大是个常规。

想一下同在多伦多的德芙林购物中心（Dufferin Mall）。在大多数日子里，该购物中心的交通人流都很平稳，它因此可能被误当成加拿大或美国的任何其他一家购物商城。但每当周四和周五的下午五点左右就会彻底变了样。成千上万外国出生的加拿大人手中挥舞着薪金支票，就像是商场内的天降奇兵，从商场的各个银行和外汇交易处汇出款项，汇给他们祖国的急需用钱的家庭成员。家庭作坊式的外汇交易处和西联汇款网点出现在了周围地区的便利店、酒吧和餐厅内，处理着汇款洪流。

说着菲律宾语、粤语、西班牙语、旁遮普语、塔米尔语、阿拉伯

语、波兰语和其他语言的多伦多人经常乘公交车、电车或地铁出行，同时看护着小孩，在一整天工作后筋疲力尽。他们得赶到商场才能向家里汇款，而且经常要排很长的队伍才能有机会把辛苦挣到的钱汇给家里。现在大多数人在智能手机上度过时间，用WhatsApp聊天、和在多伦多及国外的朋友和家人用Skype交流、玩游戏以及看视频。更多的情况下，汇款要花超过一周的时间才能到达目的地，届时收款那一头的人需要经历一次几乎同样冗长耗时的流程。

这事到底出了什么问题？每个环节都有问题。让我们找出好的那一面。必需记住：大多数排队的人使用智能手机，这是一种在加拿大广为流行同时在全球也愈加无处不在的技术工具。73%的加拿大人都拥有个智能手机，而在多伦多，这个比例几乎必然更高。这个国家的无线网络基础设施是全球最好的之一，这意味着大多数加拿大人不仅仅能够拥有智能手机（其实是台超级计算机），而且他们还能够用智能手机以两个世纪前还停留在科幻小说层面的方式来驾驭移动互联网的力量。为什么人们还用着几十年前的古老技术在一个实体网点排队汇款，而不是用他们指尖点击来汇款呢？美元的数据密度比高清视频可要低多了。实际上，根据Skype，视频电话每秒消耗500KB。⁴³发送一个比特币消耗大约500B，也就是Skype视频电话的每秒数据消耗的千分之一！

通过消除第三方中介以及极端简化流程，区块链能够最终实现即时且无摩擦的付款，这样人们就无须为了区区汇款而排上一个小时或更久的队伍、跑大老远的路或晚上冒着生命危险前往危险的地区。今天，大量公司和组织正在运用比特币协议来降低汇款成本。它们的目标是把数十亿美元给到世界上那些最穷者的手中。这些行业已被一小撮公司所控制，这些公司使用它们独特的地位和历史遗留基础设施来制造垄断经济。但它们也看到了区块链技术所带来的对它们的风险，因此害怕了。根据德勤的数字加密货币集团的领导埃里克·皮斯奇尼，在支付领域的公司目前“对于区块链对它们所带来的影响真的感到紧张。西联汇款、MoneyGram、iRemit和其他公司害怕对它们商业模式的颠覆。”⁴⁴它们应

该感到紧张，因为有一个新兴行业诞生了，那里有着崭新且颠覆性的公司想要取而代之。

好吧，卢克，我的朋友，年轻的安娜丽怎么办？

要为世界上的穷人们创建一个基于区块链的支付网络，尚有两个障碍。首先，汇款的人中很多都是收到现金形式的工资，而收款的人也都在基本以现金交易为主的经济体中。其次，发达国家和发展中国家的大部分人没有能有效使用区块链的知识和工具。虽然现金很可能将来像渡渡鸟那样灭绝，但是在发达世界的雇主开始向智能钱包贮存价值并且马尼拉、太子港和拉各斯的小型街边商店开始接受数字付款之前，我们还会继续需要纸钞。西联汇款知道这个事实，这就是它为什么至今仍然重要的原因，在全世界有着超过50万个代理点。⁴⁵如果你想要把汇款换成现金，则选择很有限。西联汇款如果只有一个代理点，则就无法换现金。它的网络让它能够在几十年里在整个市场上维持垄断地位。过去几乎从没有任何公司有一个无缝且易用的“杀手级应用”技术。但现在有了。

我们来观察一下Abra或其他像它那样的公司。用Abra这样的名字，人们可能原本预计看到点“cadabra”式的神奇变化^[2]，而这公司也没让人们失望。Abra正在比特币区块链上建立一个全球性的数字资产管理系统。它宣称的目标是把每一部智能手机都变成一个取款机，可以用来向网络中其他成员提供实体现金。我们要测试该解决方案是否改进了安娜丽的体验。

安娜丽和她的母亲的安卓智能手机里都下载了应用程序。安娜丽的起始余额是加元。一点击按钮，安娜丽就启动了向她母亲的转账。她几乎瞬间就以比索收到了转账款。此时她母亲可以选择在手机里保留比索作为一种储值，或是选择在日益增长的接受Abra付款系统的商户那里花掉这笔钱。通过创建一个支付工具和价值储存，Abra有效地取代了传统

银行系统的两个最关键的角色：支付和价值储存。光这一点就是个革命性的概念了，但真正有趣的地方在于：她母亲想要现金。她用现金付房租、买食物以及应付任何其他开销。她检查应用程序，注意到在方圆四个街区范围内有其他Abra用户。她向他们都发送了消息，看看谁能把数字版的比索兑换成实体版比索以及按什么价格兑换。这四个人把各自服务的不同开价回复给了她。其中一人收3%才提供前述服务，另一个收2%，还有两个各收1%和0.5%。她母亲决定找那个收2%的取款员——并非因为他最便宜，而是因为他有五星评级且同意在半途中和她碰面。他们然后碰了头，她把Abra系统里的比索换成了实体版的比索纸钞，而取款员则收取了佣金，随后他们愉快地各自离开。Abra则收取了25个基点（2.5）的兑换费。

从钱离开多伦多到达持有现金的菲律宾收款人那里的整个过程，只花费了一小时不到，净成本则是25个基点，包括外汇汇兑和所有其他交易成本。鉴于每笔西联汇款的交易需要最多达七到八个的中介、联络银行、本地银行、西联机构、个人代理人和其他中介，而Abra交易仅需要三个：网络内的两个对等参与者以及Abra平台本身。“我现在明白了。那真棒！”安娜丽狂喜地说道。⁴⁶

Abra若要朝全球扩展业务，则它们必需得解决两个核心难点。首先，整个网络需要临界规模数量的取款员才能让服务足够便利。安娜丽的母亲周边最近的取款员如果也相隔了20英里，那么她就不会用这个服务。Abra知道这一点，它们因此正在预先签约取款员，光在菲律宾的数量就至少有成千上万名，这些人已准备好在事情启动后就随时开展交易。第二，这个模式能否管用，取决于一个假设：取款员和客户在交易数字货币和实体货币时将会遵守承诺。这个问题倒没那么值得担心。像Airbnb、Lending Club和Zipcar那样的公司已经打破了人与人之间不会互相信任的神话。的确，对于Abra的首席执行官比尔·巴希特而言，所谓“共享经济”的公司数量的激增已经让他坚信那不是个问题。“人们乐意于互相信任的速度，比他们乐意于信任某个机构的速度要快得多”，

他说道。⁴⁷

智能手机是这所有一切的关键。智能手机让你能够向其他人出租公寓或汽车或提供搭乘服务，它也能以相同方式被用作为自动取款机。巴希特说：“神奇的是，人们愿意以共享经济的方式来做事，他们并非仅仅为了钱，但也许点对点借贷是个例外。”此外他说：“对我们来说，更重要的是你信任其他人，而不是信任Abra。如果你信任其他人，你将很可能知道Abra、喜欢上它并且有良好的体验，并很可能最终信任这个平台。”⁴⁸

Abra并不是一个汇款的应用程序，而是个崭新的价值交换的全球平台，它同等程度地综合了分布式无须信任的区块链网络、智能手机技术的力量以及人们愿意信任网络内其他参与者的人性倾向这三者。通过让用户能够用传统货币来储存价值、在网络中传输价值以及在快速增长的商户网络中付款，Abra所呈现的不仅仅是西联汇款的角色，而且是像VISA那样的信用卡网络。Barhydt说道：

西联汇款和Visa的交易结算轨道各自差别很大。但Abra的交易结算通道既用于个人之间付款又用于个人和商户之间的付款，两者完全相同……历史上第一次，我们提出了一个既能用于国内又能用于跨境、既能用于个人之间又能用于个人和商户之间付款的单一解决方案。⁴⁹

Abra可能最终会成为一个全球性的巨无霸，让世界上那些最大金融机构竖起的高墙开始颤抖。但现在它只是一个用来减轻某个全球性重大难题的很棒的简单解决方案，正在帮助一个菲律宾家庭省下那么一点成本。此外，随着汇款数额明年将会超过五千亿美元规模，这个市场机会完全不可忽视。

区块链助力人道主义援助

区块链能否在根本上改变非政府组织、政府和个人捐助者向国外提供援助的方式？数十亿美元的援助中有成千上万是每年流向了发展中国家，但援助的宏观经济效果并不总是很清晰。⁵⁰有大量证据暗示着有腐败的政府官员、当地豪强和其他中间人在援助抵达预定对象之前就早已偷走了很多。更麻烦的是，根据国际经济周刊，“政府收入的增加会减少公共物品的供给”。该报告得出结论：大量消费那些援助或意外之财并不必然导致福利的增加。⁵¹组织机构膨胀和效能低下两者结合在一起，共同导致了那些最贫穷国家中大量的浪费以及穷人和富人之间更严重的不平等。这不仅对于政府到政府之间的跨国援助是事实，而且对于那些脚踏实地在穷困潦倒的地方第一线工作的非政府组织而言，也是如此。

我们在本书介绍里粗略地谈到了外国援助的问题。让我们进一步深入探讨一下这个问题。回想一下，在2010年海地大地震的震后时期，经ProPublica（一家独立的非营利性新闻机构）进行了一项研究后，红十字会冒着危险赶来了。但美国国家公共电台却发现该组织浪费了不少资金并且很多承诺并未被兑现，例如建设13万幢新房屋的承诺。实际上它只建造了6幢。⁵²作为辩护，红十字会争辩道海地那破旧的土地产权登记簿阻碍了它的努力：没有人能查明谁拥有土地。结果红十字会因地制宜地勉强解决了问题。基于区块链的土地产权登记能否通过提供清晰的产权而改善这个情况并且也许能阻止非法征收呢？

外国援助也许在许多政府不称职以及无良中间人寻租行为的最明显例子，因此也是探讨区块链解决方案的完美理由。2010年海地大地震是过去一百年中最具毁灭性的人道主义危机。⁵³当海地政府瘫痪而危机肆虐之时，成千上万的“数字人道主义者们”汇集在互联网上帮助第一批响应者们收集、分类鉴别和图形化那些受到摧残的海地人从手机中发出的

呼救。这些临时团体最初是在网上由想法类似的志愿者们所组成的，它们在危机过程中变得越来越组织化并高效。尤其是Crisis Commons社区的确有了大不同。Crisis Commons作为一个例子，证明了一个全球性解决方案的网络，这是一个新兴的由民间社团组织、公司和个人组成的非国家性网络，协同合作解决重大问题。数字革命已经让新的网络能够跨国界的联系并协作起来，并能解决问题，让全球性合作和全球性治理得以实现。互联网对所有这些都给予了可能。对于人们在海地所创造出那种公共产品，人们在此前却从未能够共同组织创造出来过。互联网的这个信息层被证明是至关重要的——为有需要的人们和类似的志愿者组织提供关键性的联系、专有技术和数据。设想一下，如果还有一个价值层会怎样？那能够创造出什么样的可能性？

区块链能够在两方面改进外国援助的交付。首先，它能摆脱中间人作为大量援助的转移渠道的媒介作用，以此来减少由来已久的直接挪用和盗窃的问题。其次，作为记录资金流动的一份无法篡改的账本，它迫使从援助集团到各类大型机构正当行事并恪守承诺。如果它们违反，人们将能够看到它们的过错并让它们负责。

我们能够轻易得想象联合国儿童基金会或联合国的妇女项目使用区块链来给妇女和儿童直接募集资金，而无须通过当地的政权组织来做这件事。穷国的个人能够通过由不同援助团体作为网络结点而管理的分布式账本，签约申请福利。当特定的援助被交付时，比如红十字会的疫苗或联合国儿童基金会的学校物资，那些交易就能在账本中打上时间戳。这将减少或可能甚至防止援助团体不小心给某些人或社区提供双重援助，这样就能把福利援助更公平得扩散出去。

事实上，联合国儿童基金会早已开始研究数字加密货币了。2015年6月，联合国儿童基金会宣布启动了Unicoin，一个让孩子们能够“挖矿”的数字货币，只要他们向该计划提交灵感创做出的绘画。然后该币可用于换取笔记本和铅笔。⁵⁴这是一个小小的开始，但未来机会却是无

限的。紧接着就可以想象出我们在第一章中所做的假设：遍布于发展中国家的村庄里的孤儿院与联合国儿童基金会合作，自每个孩子到来之时起就为他们开立账户。捐助品将按比例分配到每个孩子的个人账户。豪强和其他腐败官员无法染指。世界上最穷和最弱的孩子们在成年时将有钱开始生活。这些都可以靠区块链来得以实现。

自然灾害的救济或为穷人提供物资当然无法总是点对点提供的。经常的情况是，机构的参与不仅仅是值得的，而且也是必需的。但区块链能够大幅度提高这些组织和其他机构在外国援助价值链中的透明程度以及功能。向红十字会捐献的每一美元自开始在价值链上传递直到到达直接受益人，在整个过程中被一直追踪到。回想下我们在第一章中假想的场景——红十字会可能为其每一项最重要的项目都发起众筹活动——提供医疗援助和阻止疾病扩散、水净化、房屋重建——当你捐献时，你就知道捐的钱是否变成了一块木板、一加仑水或一片邦迪。如果资金失踪，社区将知道，并能够让这些机构承担责任。让援助团体们自行承担责任的智能合约将被使用。大型项目——从住房计划到水净化项目的实施——其资金可以直接进入第三方监管账户，且只有在成功完成某些关键节点后才能释放发放出来——这些节点可能包括获得了场地的产权、进口了原材料、与当地供货商签署了合同、做出了成品、安装了特定数量的净水取水点。那么这会产生什么样的结果呢？在外国援助的交付过程中大幅度提高了透明性和可追责性，因此最终结果也得到了极大改善。

外国援助是发达国家向发展中国家的第二大资金流动，仅次于汇款。区块链技术能给那些慈善性非政府组织带来透明性、可追责性和更高效的运营，以及能促使在危机和正常情况下更好地提供关键服务。当然，的确存在不少执行层面的挑战及必需克服的困难。第一线工作的人们需要知道如何使用这些技术。移动电话网络可能在危机发生时中断。手段高超的犯罪分子和不良机构也许仍能找到欺骗穷困人群的办法。但这些就是不去探索新技术的理由吗？当然不是。今天的形势是不正常

的，在很多情况下就是完全崩溃的。赋予个人以权利、让援助团体承担起责任，意味着更多援助会达到正确的人手中。减轻贫困和解决灾难危机是通往全球性繁荣的梯子的第一根横杆。让我们给区块链一次机会吧！

小微金融：微微支付的点对点援助

小微金融是一个超越了金融服务和发展援助的行业。不像那些自上而下给予的援助，小微金融机构（MFIs）试图让人们储蓄、投资和开办小型企业。更多情况下，它们采取社区储蓄合作社的形式，在那里社区成员能够共同归集资金成为资金池，并贷出给其他人满足短期融资之需。只要适当地执行并管理，小微金融网点能够为困苦社区带来真正的福利：它们减少长期饥饿、增加储蓄和投资，并在很多情况下帮助了妇女。⁵⁵

然而小微金融机构今天存在着问题：首先，对它们如何运营的，几乎没有监管，它们偶尔会创造出掠夺性贷款以及胁迫性催收方式，压榨社区并让后者更加绝望。其次，鉴于前述这点，发展中国家的政府已经发现，抑制不良行为的最佳方式是取缔或严格限制所有的小微金融机构，就像印度在发生了一次关于小微金融机构的争议后于2010年所做的那样。⁵⁶第三，资金并非总是能到达正确的去处。没有什么办法能确保最需要钱的社区成员获得钱。第四，小微金融机构仍然在很大程度上是区域性的，这既限制了资金规模，又限制了投资及储蓄的机会。

所以从事于解决贫困问题工作的人们会自问：区块链到底能够在这些组合工具中的哪一项上发挥用场？它能怎样改善我们所做的一切？

首先，它将改善行政管理的可追责性。就像公司透明度问题一样，捐献者将被吸引至任何使用区块链技术因此更透明更负责的非营利机构。此外，如果小微贷款纪录于区块链上，并且小微金融机构的客户们

被允许访问检查前者，那么客户们就能让这些机构对坏事承担起更大责任来。如果未来的借款人或储户能选择公开透明的机构，谁还会去选择那些封闭不透明的吗？

其次，它意味着更好地保护妇女和儿童。通过智能合约，资金可以捐献给第三方监管账户，只有妇女才能够访问该些账户，比如用于买食物、女性用品、医疗用品和其他必需品。男人不能取走钱去买烟酒或用于赌博，后者对于储蓄或小微金融的资金而言可能是个持久性的问题。

第三，它能让人们从全球范围内获取资金和机会，并将吸引全球的捐助者。社区要使用哪个小微金融机构，通常被地理位置所局限着。今后，未来的借款人能够上网从一系列潜在贷款人中获取最佳的出价，从中发现最好的利率、条件和声誉。正式的小微金融机构将当然会继续存在下去，但也有更简单的方式通过区块链来联系其他对等的人，这会使得小微金融机构不再那么必需了。

最后，区块链支付通道，例如比特币，基本上是为小型、缺乏权利的借款人而量身定制的，让他们能用上小额支付（我们把它叫作“微微支付”）并把成本降低至接近于零。在一个每分钱都很重要的世界里，用户能够归还贷款、提取资金和小额增加储蓄，所有这一切在区块链产生之前的世界里都面临大得多的挑战。世界上虽然存在很多凄惨贫困的地区，但手机渗透率和互联网连接也正在变得商品化，考虑到这点，人们也应当能够迅速有效地做到微支付。

像家一样安全？通往资产所有权之路

土地产权登记是被赫尔南多·德·索托称之为非市场性交易的东西，一种通常牵扯到当地政府的经济交换。非市场性交易成本包含了排队等待的资源浪费、追溯产权、完成和备案文书、办理官方流程手续、解决

争议、给某些官员和审查员好处等等。⁵⁷在穷国中，体制虚弱，有些政府官员也广为人知地行为不端，故前述成本是个高耸的壁垒障碍。洪都拉斯是这样一个地方：中美地区第二穷的国家，收入分配极端不平均。2008年的经济危机阻碍了汇款流入，而2009年的一场军事政变则罢黜了民主选举出来的曼努埃尔·泽拉亚。此次政变由该地区最大的地主之一所支持，他是一个靠早期胁迫农民出售土地产权而豪夺土地发了大财的棕榈油大亨。⁵⁸

自从1990年中叶起，世界银行和其他全球性非政府组织⁵⁹已经向洪都拉斯投入了1.253亿美元以及技术资源，来设计和管理能够加速其发展的土地相关的开发项目。⁶⁰我们曾看到一些计划要设立空间数据基础设施，能够支持土地和自然资源的产权与使用、气候和自然灾害以及社会经济状况的数据的图像地理标签，大城市可以以此来提供战略规划和投资的信息。还曾有过提到把土地项目的数据库和环境与灾害管理项目的数据库在其国家和地方层面进行整合。⁶¹这些计划真是雄心勃勃。

问题在于，在财产登记、土地出售和争议解决领域，其仍然被声称遍布着腐败，包括对中间人、法官和当地官僚的谴责。根据美国贸易代表处，其财产登记系统仍然高度不可靠。⁶²由于政府把世界银行的辖区限制在市区，在住宅的土地产权登记期间，其农村的家庭被系统性地忽略了，而土地通常是他们最有价值的资产。其农村地区手无分文的农民至少能从土地管理计划中受益。自1998年以来，至少洪都拉斯的农村贫困减少了。在所有发达国家中，模糊不明和腐败问题在产权争议中被暴露出来了。如果洪都拉斯遭受一次象海地在2010年所遭受的那种巨大自然灾害，红十字会那样的援助组织在理清产权这团乱麻时会同样受阻，以至于难以交出安全耐用的房屋。

如果有一个普世的总账能够囊括所有这些数据并且能把信任注入一个极其缺乏信任的局面，则会发生什么？“区块链看上去似乎特别擅长

于处理交易，而其他系统则都不必然擅长处理这个”，德索托说。“事实上穷国在本质上就极为腐败，因此把你的交易账本通过安全流程措施保存在每个节点，这将会使系统高效、便宜且迅捷，并且这也是穷人们想要的结果，因为这保护了他们的权利。”德索托补充说。⁶³这系统是这样运作的：区块链是一个公开的总账，意味着它能够保存在那些需要查阅它的洪都拉斯政府官员的电脑桌面上，也能保存在输入数据的现场工人以及想要留存副本的公民的移动设备上。区块链是个分布式账本，意味着这几方都不能拥有它，而它又是个点对点的网络，意味着任何人都可以访问它。在洪都拉斯这种公共机构的可信度很低而产权体系又虚弱的地区，比特币区块链能够帮助恢复信心并重建声誉。

这就是位于德克萨斯州的初创企业“公证通”计划与洪都拉斯政府合作共同要做的事情，并因此与Epigraph（一家产权软件公司）建立了合作伙伴关系。“公证通”的总裁彼得·柯尔比说：“这个国家的数据库基本上被黑了。所有官僚们能进入数据库，为他们自己先挑到最好的财产。”他又补充说，大约60%的洪都拉斯土地是没有正式记录的。目标是在区块链上记录下所有的政府土地产权，而首个试点项目将在2015年年底完成。柯尔比告诉路透社，洪都拉斯通过采用“公证通”的区块链技术，能够让它历史遗留下来的系统弯道超车超越过发达国家所用的系统，这能最终有助于实现更安全的抵押和采矿权。⁶⁴“从专利权到房屋所有权的文档只有在特殊情况下才是纸质的，除了历史原因外它们没有理由应当是纸质的。在任何涉及产权和时间问题的交易或互动行为中，区块链都能发挥作用，”⁶⁵考西克·拉戈帕尔说道，他是麦肯锡的硅谷办公室以及支付业务的负责人。

截至今天我们不知道洪都拉斯政府是否会执行土地产权登记在区块链上，或是否会在试点项目之后继续维持使用。在以前对土地登记的尝试中，政府已经逐渐不再承担系统扩充升级和纳入更多人口的成本增加。但是如果账本能提供可靠、无法篡改的数据，那么非政府组织就能

够获得额外的数据，用以向政策制定者和治理者进行传达并对之施加影响。如果它消除了目前洪都拉斯土地登记所需的六个步骤中的五个，并把时间从22天缩短成10分钟，那么那些非市场性的交易成本将会降低到接近于零。⁶⁶对于大型全球性公司在环保指定区域、农民或土著人世代居住区域购买土地、建造建筑、获取木材或水却又不给予公平的补偿，也许区块链让记者和人权分子能够迫使大公司出于羞愧而停止做那些事。我们对此抱有很大希望！

实施层面的挑战和领导机遇

区块链技术显然不是世界经济和金融困境的万能解药。技术并不创造繁荣；人才是繁荣的创造者。存在需要克服的障碍，也存在着领导的机遇。首先是技术方面的。根据国际电信联盟的数据，互联网连接仍然有巨大的缺口，要么是因为电信基础设施薄弱，要么是因为服务太贵无法负担。⁶⁷

其次是文化水平。使用智能手机和上网需要一个可行程度的文化水平。在美国，18%的超过16岁的成年人的阅读能力低于第五等级，30%数学水平较低，⁶⁸而这些成年文盲中43%的人生活贫困。⁶⁹发展中国家中的文化水平分布十分不平均。非洲的许多地区，识字率徘徊在50%左右，而如果比较男女间差别，则问题又更加严重。例如在阿富汗、尼日尔、塞拉利昂、乍得、莫桑比克和其他穷国，男女之间的识字率差距令人震惊地达到了20%。⁷⁰

第三是道德问题。区块链一个强大的工具，但就像所有技术一样，它并非是天然地好或坏。人们能够利用那些非凡的技术，从电力到无线电到互联网，用以实现善意或恶意的目的。社会中能够为了善的目的而运用区块链技术的机构，比如援助团体、民间社团组织、公司和政府，

我们需要它们的领导来约束连接入这一巨大网络的个人。只有当这些挑战被克服时，区块链技术才能发挥出它的潜能，成为全球繁荣和积极变化的工具。

[1] 桌面游戏“大富翁”中的一张机会卡——译者注

[2] abra和cadabra合在一起是魔法咒语的意思——译者注

第八章 重建政府和民主

爱沙尼亚共和国是个波罗的海国家，南临拉脱维亚，东临俄罗斯。它的人口有130万，比渥太华的人口略少。¹当爱沙尼亚在1991年从苏联重新独立出来时，它有机会彻底重新思考政府的角色并重新设计其运作的方式、提供的服务和通过互联网技术达成目标的途径。

今天，爱沙尼亚被普遍视为是数字政府的世界领导者，其总统托马斯·亨德里克·伊尔韦斯将成为第一个说出此话的人：“我们为我们所做的而感到自豪”，他告诉我们，“我们希望世界其他地方能学到我们成功的经验”。²

爱沙尼亚在个人和政治权利方面的社会进步指数上排行世界第二，与澳大利亚和英国并列。³爱沙尼亚的领导人已围绕去中心化、互联化、公开性和网络安全而设计了他们的电子政府战略。他们的目标已定位于那些不会过时的基础设施来适应新的发展。所有居民能够获得网上的信息和服务、使用数字身份来开展商业活动以及更新或纠正他们的政府记录。爱沙尼亚的工作中很大部分是在区块链出现之前就有了，它引入了无须密钥签名的基础设施，这能与区块链技术完美地整合在一起。

电子版爱沙尼亚的模式的核心在于数字身份。截至2012年，90%的爱沙尼亚人有数字身份证来获取政府服务并在欧盟内通行⁴。嵌入在身份证里的芯片含有卡主的基本信息以及两个证明，其中一个用来验证身份，而另一个用来提供数字签名，此外还有一个由卡主自己选择的个人身份识别号（PIN）。

爱沙尼亚人使用上述东西来投票、审核和编辑他们的网上自动化税

务表格、申请社保福利以及获取银行服务和公共交通。这个过程并不需要使用银行卡或捷运卡（Metrocards）。爱沙尼亚人也可以用手机上的移动身份证来做这些事。在2013年爱沙尼亚人提交的税务申报超过95%是电子方式，超过98%的银行交易是网上操作的。

在爱沙尼亚，学生和学生家长用电子学校来追踪作业、课程、分数并与教师们协同工作。爱沙尼亚实时地为每个公民把来自各个渠道的各种各样的健康信息整合进了一个单一的记录之中，所以这些记录并不单独地保存在一个单一的数据库里。每个爱沙尼亚人有独家访问权来查阅他自己的记录，也能够决定哪个医生或家人能够上网查阅这些数据。⁵

自从2005年以来，公民们已使用电子投票来进行国内选举。爱沙尼亚人使用他们的身份证或移动身份，能在世界上任何地方登录系统并进行投票。2011年的议会选举中，公民在网上投了几乎25%的票，而上次议会选举的网上投票率只有5.5%。人们显然喜欢并信任这个系统：2014年欧洲议会的选举的投票数再次上升，分布在98个国家的投票者中有1/3是在网上参与投票的。爱沙尼亚内阁使用了无纸化的流程，所有的立法草案均在网上可获取。每周内阁会议的平均时间从大约5小时降到了90分钟以内。⁶

爱沙尼亚人有电子土地登记册，其从不动产市场转型而来，把土地转让的时间从3个月缩短到了一周多点。⁷在过去几年间，爱沙尼亚已启动了“电子居住”计划，世界上任何人均可申请一个“跨国数字身份”并进行验证，以此获得安全的服务以及数字化地对文件进行加密、核实并签署。全球任何地方的企业家均能在20分钟内在线注册其公司，并在线管理该公司。这些能力促成了爱沙尼亚作为一个数字化国家的形象的建立。⁸

若没有扎实的网络安全，上述这些功能均无法实现或被接受。安全技术公司Guardtime的首席执行官迈克·高尔称：“数据完整性是网络世界

的首要问题，爱沙尼亚在十年前就认识到了。它们建立了这项技术使得政府网络上的所有东西无须对人给予信任就能被核实.....政府现在不可能欺骗它的公民。⁹”

爱沙尼亚的网络安全来源于它的“无私钥签名基础设施”（KSI），该设施以数学方式在区块链上验证任何电子行为，而无须系统管理员、密码学私钥或政府工作人员。这一能力确保了彻底的透明性和可追责性，权益人可以看到谁获取了什么信息、在什么时候获取以及对方用它做了什么。这样，国家能够证明记录的完整性以及监管合规性，而个人则无须第三方介入就能够核实他们自己记录的完整性。该设施降低了成本：没有私钥需要保管，也没有文件需要定期重新签署。根据电子爱沙尼亚网站，“只要有KSI，历史就无法被重写。”¹⁰

显然，区块链技术不仅仅适用于逐利的公司，也对那些致力于造福所有人的公共机构所适用，无论是政府、教育机构和医疗机构，还是电网、运输系统和社会服务。那么从哪里开始呢？

有些方面还待完善

1863年，美国总统亚伯拉罕·林肯在葛底斯堡的一场演讲中说，社会最崇高的目标就是“政府为民所有，为民所治，为民所享”。120年后，罗纳德·里根总统在1981年就职演讲中说：“政府并不是问题的解决方案，政府就是问题所在”。区块链初期生态系统中很多人都同意这一说法。2013年一场研究调查显示，超过44%的比特币用户承认他们是“自由主义者或者自助性组织资本主义者”¹¹。

各行各业的自由主义者都倾向于支持比特币。它是去中心化的，并且不受政府管制。它采用匿名形式，很难确定收税标准。在稀有性上，它和黄金相似，而自由主义者偏爱黄金标准。这是一个纯粹的市场，由

供需驱动而非依靠量化宽松政策。因此，也难怪兰德·保罗会成为2016年总统竞选中，第一个支持用比特币支付竞选经费的候选人。

自由主义的倾向让数字货币的反对者有了完全抵制区块链技术的素材。吉姆·爱德华兹是英国商业内参的创始编辑，他曾描写过一个自由主义者眼中的天堂，这是一个类似索马里的国度，“相关部门干预少之又少，市场也不受繁重的法律与赋税约束。”他将这个天堂描述为“一场噩梦.....整个世界是极度不稳定的、混乱的，老板级别的犯罪分子越来越多，他们随意暗杀自己看不惯的人，财产大批量地转移到小部分人手里，这一小部分人占人口的比例甚至比当前美国占总人口1%的特权人群所占的比例更低”。[12](#)

当然，我们所居住的，是一个危机四伏的世界。人权观察组织（于20世纪70年代成立，致力于支持公民团体）执行理事肯尼思·罗思写道：“世界上还没有一代人经历过这样的混乱场面。之前的曾出现过的阿拉伯之春给世界各地带来了冲突与镇压”，“许多政府在应对这场混乱中，要么轻视人权，要么彻底放弃人权”。它们利用互联网来监视公民，利用遥控飞机朝平民投掷炸弹，还关押大型公共活动中的抗议者。[13](#)

秘鲁著名经济学家赫尔南多·德·索托表示，这种处理混乱的方式是错误的。“阿拉伯之春从本质上来看，它仍旧是一场企业家革命，因为他们的资产被剥夺征用。从根本上说，这是一场对抗现状的反叛运动”。而现状就是持续不断的征收，政府反复践踏公民的产权，直到他们再无选择，只能在体制之外寻求谋生的办法。[14](#)

因此，进一步的践踏权利是最糟糕的应对方式，因为这一举措会逼得更多人在体制之外寻求解决方案，这包括记者、机会主义者以及企业家。过去20年，西方民主政治的投票率锐减，包括美国、英国、法国、德国、意大利、瑞典以及加拿大。尤其是，年轻人也在寻找机会实现体

制外的社会变革，当然，绝不是通过投票实现。大多数美国人认为，国会的职能已经衰退，而其腐败程度甚高。这种判断是有依据的：和许多国家一样，美国政治家是为有钱的政治献金捐赠者和利益集团服务，然后国会的很多成员成为了说客。有一个明显的例子：92%的美国人都希望对枪支购买人员进行背景调查，但是有钱和有权的美国步枪协会，会阻碍任何致力于改变现状的立法活动。“民有、民治、民享的政府”不过如此。

很多公民并没有感受到政治机构在反映他们的意愿和支持他们的人权。这些机构越是滥用它们的权力，公民越是质疑这些机构的合法性和相关性。政治社会学家西摩·马丁·利普塞特写过关于合法性的内容，他表示“是一个政治体系引导及维持这种信仰的能力——即让人相信现有的政治机构对社会来说是最合适的”。¹⁵现在，越来越多的年轻人试图通过政府及民主之外的措施来促进改变。人们在车尾贴的标语“别投票！投票就是在怂恿他们”讲述了这个故事。

“对个人而言，他们或许并不期待有可供搜查与验证的数据库来记录历史，因为这会帮助政府利用或征服人民”，赫尔南多·德·索托说道，“世界上许多国家的立法根本不完善，也是非常不友好的，进入法律体系的成本对穷人来说是完全没有意义的。对一个国家而言，如果有太多穷人和游离在系统外的人，那么就会出现很多问题。”¹⁶

随着合法性的减弱，那么自由主义也就顺势而起。但这不是对困扰政体问题的解决方案。在这个麻烦重重的世界中，我们需要强大的政府，我们需要高绩效、有效率、反应迅速及对公民负责的政府。

那么政府应该做什么呢？赫尔南多·德·索托在《华尔街日报》中写道：“要建立、简化并加强让资本主义繁荣昌盛的法律与结构。正如每个在利马、突尼斯和开罗的街上走过的人所了解到的那样，资本不是问题所在，资本是解决方案”。¹⁷那么问题又是什么呢？“得到人们的认同

是问题所在，”他告诉我们，“政府无法强迫人们进入体制内部。因此我认为，现在世界各地的政府都会愿意改变体制。”¹⁸

这就是区块链的切入点。区块链的设计理念可以推动这种转变，因为这一技术能够支持且实现下述更高标准：

正直。为了重建公众对政治机构的信任，民选官员必需正直行事。信任必需从体制内做起，体现在每个操作流程中，而不依赖于任何一个人。由于区块链支持极高的透明度，所以重建利益相关者与代表之间的信任变得越来越重要。持续的透明性对维护这种关系来说至关重要。

权利。每个人都有直接或通过投票来参与政府事务的权利。无论是谁当选，都必需作为人群中的一员光明磊落地处理事务。公民通过互联网承担了更多社区责任，从民选官员中得到信息并对其产生影响，反过来也一样。通过区块链，公民还可以做到以下这点：他们还可以倡导，倡导将政府行为以公共记录的形式封存在一个不可改变、不能收买的账本上。这不仅可以用于少数有权者的制衡，还能用于在更广泛层面达成共识，如让潜在的美国枪支拥有者接受背景调查。

价值。选票必需具有价值。系统必需为所有利益相关者设定激励机制，要对公民而非大大资本负责，并恰当地使用税收。政府的运作模式必需通过技术实现更高的绩效、更良好的运作及更低的成本。

隐私与其他权利保护。不监视公民，不随意干涉公民隐私、家族或家庭，不攻击任何人的荣誉或声誉。不在没有补偿的情况下恣意攫取财产，这包括房产或发明专利之类的知识产权。不审查新闻组织，不干涉集会自由。人们可以在区块链上私下、匿名地登记版权，组织会议并交换信息。要注意任何声称在个人隐私与公共安全之间做出取舍的政治家。记住，这种取舍就是错误的二分法。

安全性。每个人都平等地享有法律保护，且不受歧视。不应该存在随意拘留或逮捕的行为，也没有个体或团体需要生活在政府或执法机构的恐惧中。不需要因为种族、宗教或出生国家而受到这些机构的成员残酷、无情或可耻的对待。警员不能扣押非法动用武力的证据，这些证据不应该遗失，并且都可以在区块链上记录并追踪到。

包容性。使用互联网，公民可以参与到其中，并从别人那里了解更多知识。通过区块链，系统可以降低成本，提高效率，让所有公民都参与进来，在法律面前大家都是人，并且可以平等地享受公共服务（如医疗和教育）及社会保障。

技术是一个强大的工具，但是单单依靠其本身是无法实现我们所需要的改变的。本着“未来不是让我们去预测的，是让我们去实现的”这样的精神，让我们一起为一个具有合法与信任的新时代而重塑政府吧，是时候停止胡乱的修补了。

高性能政府服务与运作

关于“大政府”的批评从某个意义来说是正确的。谈到效率的时候，政府的服务和运作流程还有很多需要改进的地方。有些政府是孤立的组织，他们不会分享信息。而官僚主义总是会胜过常识或共享实践。公民很少能享受到一站式的政府服务。不少国家都流传着数不清的关于政客和官僚滥用税款的故事。

区块链可以改善客户服务，提高效率，在完善结果的同时，保证政府诚信透明。它对增强政府各方面性能来说非常重要，而有些对发展中国家和地区来说尤其重要，在这些地方，政府正在创建新的流程，区块链可以帮助他们实现系统升级，建立长期稳定的开放式政府。

我们可以先从区块链应用的两大领域入手：综合政府以及公共领域的物联网使用。

综合政府

爱沙尼亚正在提高行政效率，并为居民及商业提供综合服务。他们要为每个人建立一种电子身份证，使用区块链支持的名为“X-road”的互联网主干网，来连接公共部门和私营领域的多个程序与数据库。其他人也可以这么做。

许多国家，像加拿大、英国还有澳大利亚，都明确拒绝将中央人口登记和单一政府ID（身份）作为公共政策。这一决定源自对个人隐私的关注，以及对国家权力不断扩大的厌恶，尤其是在授予或撤销身份时的权力。

但是，正如爱沙尼亚的情况，如我们将现存于多个数据库的官方文件（比如护照、出生证、结婚证、死亡证明、驾照、医疗卡、地契、选民身份证、商业登记、纳税情况、就业数目、学校成绩单等等）进行哈希运算并记录在一个区块链上，那么这个基于区块链的网络就可以在不依靠任何中心化流程的前提下提供综合服务。这个模型不仅可以保护隐私，它可以让人们对信息的准确性进行验证，并且看到谁访问或添加了信息（比如一个永久信息的审核），从而进一步加强隐私。

实际上，在未来让每个公民都持有自己的身份信息而非政府持有，这一点是有道理的。正如我们在第一章中解释的那样，就和网络和集体协作能够消除对政府发行货币以及银行建立信任的需求一样，未来人们甚至不需要政府来发行身份证。加密安全公司WISeKey的卡洛斯·莫雷拉说：“如今，你需要授权组织来提供身份，比如银行卡、频繁飞行积分卡或者信用卡。不过这个身份现在就是你的了，而世界范围内互动所产生的数据，则由其他人所有。”¹⁹在区块链上，个人持有其身份。你

的“个人化身”可以在你的指导下，决定向谁公开哪些信息。它还可以做出关于集成数据的选择。但是，并不是你所有与政府相关的信息，都会整合到一些大规模政府数据库中，整个整合过程是由你在虚拟世界的身份所控制的，而这个身份最终是由你所有并控制的。

更完善的整合方案会对与生活相关的事件（如婚姻）带来支持。梅拉妮·斯旺是区块链研究学院的创始人，她解释道：“区块链适应安全身份、多重合约及资产管理等需求的架构，使得它在婚姻事务上有着很理想的用途，因为一对夫妇可以将婚约与共享储蓄账户、儿童医疗合约、地契以及其他与相关文件绑定在一起，以谋取一个可靠的共同未来”。有些人认为区块链技术可以成为一个无须相关机构批准或参与的公共文档登记中心。2014年8月，佛罗里达的迪斯尼乐园见证了世界上第一个用区块链记录的婚礼。这可是智能婚约啊，懂了吗？[20](#)

除了综合服务，政府可以在保持透明性和可靠性的前提下注册和管理文档。试想一下，发行、验证、更新、恢复并替换人们的官方记录需要涉及很多的工时。除了确保文档的精确性外，区块链下的登记系统可以通过点对点网络来支持自助服务及个性化服务。在自助服务中，人们可以借助网络来验证文档，而不再需要登记员的帮助。而个性化服务中，当你生成官方文件后，它会自动包含你的相关信息及其访问权限，并且在文档元数据中追踪信息的访问者和使用者。

举个例子，英国政府正在调查区块链在维护众多记录中的应用，尤其是它对记录完整性与正确性的作用。保罗·唐尼是英国政府数字服务中心的一位技术架构师，他表示，完美的登记系统应该“可以证明数据不被篡改”，还应该存储所有变化的历史情况，并且能“公开接受独立检查”。[21](#)

基于区块链的系统，能够提高各类文档登记及其他政府流程的效率及诚信度，我们可以将供应链管理同物联网结合起来，来标注一个新的

智能芯片，用来沟通记录来源、所有权、保证书或特殊信息。政府采购办事处可以追踪物件，并且实现每个步骤的自动化：采购、打款、支付销售税、更新租约或订购升级。这能够完善资产管理，减少纳税人行政费用，同时还能增加政府收入。²²

更有意思的是在国家和所在地区里存在的机会：将不同的区块链网络连接起来以在多个辖区实现更高的效率。比如，机动车辆部门可以连接全国或省界驾驶员数据库，来创建一个虚拟数据，从而帮助确认驾驶员身份、现状及并追踪记录。还有在美国医疗保健系统里，梅拉妮·斯旺称：“假如病人、保险公司、医生还有政府付款人都能将其财务状况集中到一个账本上，并且所有人都可以看到任何一笔交易状况，其透明性将可以大幅度地增加效率。”²³

公共物品联网

我们已经写了物联网上的公共交通问题。或许对政府来说会更容易用到物联网：在区块链账本上记录智能设备，来进行资产的生命周期管理，包括大楼、工作与会议区域、车队、电脑以及其他设备。借助BAirbnb，政府雇员可将供应和需求高效地匹配起来，还能通过自动化访问、采光及温度控制，来减少安保、维护以及能源的成本，并追踪政府车辆的地点、维修情况以及性能，同时观测桥梁、轨道以及隧道的安全问题。

在基础设施管理、能源、废弃品以及水资源管理、环境监控以及应急服务、教育、医疗等领域，公共账本还能带来更好的公共成果。除了改善效率，这些基于区块链的应用程序也能加强公共安全与健康，缓解交通堵塞情况，减少能源消耗以及能源浪费（比如管道泄露），当然这些还只是其好处的一部分。

安全基础设施

爱沙尼亚政府同私有部门及其他利益相关人员建立了合作，通过这一明智的举措，他们已经创建好了一个公共领域的基础架构，从而让公民更好且更方便地接触政府、银行、公共交通以及其他服务。除了这些便民服务，爱沙尼亚也在全球经济中获得了竞争性优势，为国家吸引了商机与投资。

政府也为邻近的辖区提供服务（比如消防车和急救车），向其他辖区提供外包（如数据处理），代表另一辖区提供服务（如联邦政府代表国家及省级或州政府，来处理所得税），还有提供共享服务（比如共享办公楼）。

爱沙尼亚的电子居民服务非常有用，世界任何地方的人，如果需要正式身份来启动一项业务，尤其是在线业务，都可以通过这个系统。爱沙尼亚正在努力为外国公民提供他们国家具备的服务。尽管现在可得到的服务还很有限，但是对其他政府服务最终实现端对端数字化来说，是没有限制的。比如，对当地居民免费开放的公立图书馆，可以为世界各地的非居民与学者开放电子版本的浏览权限，并且收取小额费用。那么其他类似的服务还有哪些呢，尤其是在那种数据管理和正直性在其中非常重要的数字服务领域？

超越国界来提供政府服务总是伴随着监管方面的障碍。不过，当今世界日益紧密相连，许多重大挑战并不只存在于某一辖区。全球问题的解决需要新的模式，需要其他利益相关者共同努力。那些将边境视为具有可渗透性的政策与区块链（如物联网相关）等技术结合，能够更好地解决重大而又棘手的问题。

赋予公民权利，服务自己，服务他人

由区块链驱动的网络能够让政府服务更加稳健，反应更加快。自助

服务，从恢复获得官方文件的许可开始，将大大改善政府的运作方式。政府可以通过节约时间、减少贪污腐败或其他人为障碍出现的可能，提供在线自助培训模块，及时支付公民社会保障金等等，来赋予公民权利。

从更多定义来讲，新的模型能够赋予人们权利，让人们共同参与到公共政策目标的实现中。通过区块链，我们能够达成一个全新且适度的平衡，既满足了政府管理预算、履行责任的需求，又满足了个人及团体控制、贡献预算的需要。有些辖区一直在寻找新的模型，改变之前由公务员掌控预算的情况，让个人（如多个政府规划的受益者）或社区（如居民区），甚至是所有人（如整个城市的人）都能够参与其个人预算的管理中。

比如，它不要求每个人都带着自己的标准（比如收入、资产、孩子的数量和年龄、住房类型、教育水平等），去适应各种福利不同的政府规划，相反，政府平台会根据身份、存储信息以及生产消费模式（包括风险因素：贫困地区的居民、教育水平以及烟酒和加工食品的购买率等），实现预算的个性化安排。之后个人就能决定如何利用这些资源，来根据个人情况，实现个人目标。

设想一下，你不用再为了孩子过冬的新棉袄，去劝服一些官僚人员，你可以直接自己来决定这件事！个人的责任与权限会因此增加。在社区水平（比如与社区特定服务相关的部分预算，如公园和社区中心），或在政府水平（比如建立优先性，再使用弹性预算），我们都能去做相同性质的事情。

有些辖区已经赋予了弱势群体相应的权利。²⁴区块链能够加快这一进程，让纳税人看到他们所付税款的动向，了解市民如何使用这些资源，并且确认规划是否达成目标（如改变收入、实现教育目标、找到住房等等）。这一平台会减轻甚至完全去除耗时且复杂的后台监控与报告

流程。虽然这种通过点对点网络的大范围数据记录与追踪技术，听起来有点吓人，也有点奥威尔（即受严格统治而失去人性的社会），不过实际上并非这样。与那种将所有的数据和权限依托于一些中心化权力机构或匿名官员手中的做法不同的是，个人和社区可以根据可校验的、可信的信息来行事。现在我们可以解决两个之前看起来矛盾的目标了：通过更多信息与内容来实现“政府更多的参与”；同时通过为个人和群体决策及相关的行事方案提供信息及更完善的工具，实现“政府更少的参与”。

流媒体传输开放及可信任的数据

佩里安·博林，是数字商会的创始人，她就支持分布式账本开放政府会带来好处这个观点，对她而言：“区块链能够实现彻底的透明，因为它为每个人都提供了可证明的事实。任何人都可以浏览到所有在区块链上进行的交易记录。”²⁵

政府可以轻松提供数据，而其他人则可以利用这些数据来实现公共或私人的积极发展。这和所谓的“信息自由”立法是不同的，信息自由的话，公民有可能会要求访问重要政府信息。而这个则包括资产的公布——真实的数据。政府可以以原始格式，省去个人标识，公布几千个数据类目：包括交通模式、健康监控、环境变化、政府财产、能源使用、政府预算与开支、报销账单等。公民、公司、非政府组织、学术团体以及其他人员都可以分析这些数据，将它们录入应用程序中，进行映射，或者利用这些数据来了解消费者人口趋势，了解人类健康研究模式，或者确认公共汽车是否会准时到站。

自2015年8月起，美国政府已经在其公开政府网站，公布了16.5万个数据组及工具。²⁶ 美国政府的理论是，政府持有的数据是公共数据，这一点让其成为政府透明化进程中的先行者。其他政府也紧随其后。自2015年8月起，英国政府也公布了2.2万个数据组。²⁷

通过区块链点对点网络来公布数据，将实现更高层次的效率、均匀性、实用性以及信任度。公开数据是对确保数据准确性的一种激励。人们可以浏览数据，如果发现错误，或者能够证明数据已经被篡改或毁坏时，他们还可以打上标记。

如果你在区块链网络中登记了一个完整的数据集，那么网络就可以在上面记录数据集发生的增量信息及内容的改变，并且可以阻止任何数据篡改行为。这个模式下不需要中心管理员。政府可以公布更多程序数据来帮助公众及分析师了解这些程序及其影响。

携手共创公共价值

仅仅通过可获取的可靠信息就能产生可观的经济社会价值，而个人及社区也能享有更多权利来改善生活水平，这些我们已经见证到。区块链驱动的点对点网络将会要求我们，重新考虑如何在创造公共价值的过程中划分职责。当政府公布原始数据的时候，就化身为公司、公民社会以及其他政府机构与个人自行组织、创建服务的平台。现在我们已经使用了好几年“为成功付费”的模式，来借助商业方式解决公民问题。比如，美国劳工部门就资助了一些项目，来聘用刑满释放人员，减少再犯罪情况，此外美国芝加哥市还提高了弱势群体学龄前儿童的教育水平。[28](#)

这个模式也鼓励了创新发展，此外它还提供了一种奖励机制，即通过释放资金，只有目标达成且结果可观的人，可以得到奖励。设想一下，对社区负责可持续能源方面工作的小型非营利团体来说，持续小额付款是多么重要。政府计划可以将资助与消费水平的实际下降挂钩。而非营利团体可自行申请退款补偿，不再需要依靠复杂的书面工作，而且根据政府对“为成功付费”模式的参与承诺，他们甚至可以进行融资。

将社会智能合约同政治声誉绑定

比特币网络采用区块链技术来持续地确保支付记录的正确性和完整性，与此相似，政府网络也能采用区块链来保证交易诚信、记录诚信以及决策诚信。官员无法“背着账目”隐瞒支付记录，或者其他政府记录，包括电子邮件、决策日志以及数据库。在通常情况下网络安全都是通过电子栅栏、防火墙，或周界防范来保障，而区块链则能同时从内部和外部提供保护，防止篡改。这样一来，它就能让“诚实的人继续诚实”。[29](#)

透明度对改变机构行为来说是至关重要的。当然，我们不能强迫这些公众代表，去遵守这样的价值观和行为，不过我们可以通过智能合约，来限制他们的决策与活动。这种智能合约会规定他们作为代表所担负的角色与责任，然后在区块链上密切关注他们的行为，并进行评估。

记住，智能合约是自行执行的协议，它存储在区块链上，没人能够控制它，所以每个人都可以信任它。像大老党（即美国共和党）这样的政治势力就可以采用智能合约，防止唐纳德·特朗普这样借助党内基础设施在预选中辩论、竞选的候选人在普选中作为独立候选人出面。我们可以将智能合约运用到不同的政府运作中（比如供应链、外部法律服务、已履行合约支付），甚至可以运用到更复杂的政府角色及民意代表中。我们确实可以预见到，点对点网络将追踪到被选举官员的承诺及其履行情况。监察机构已经在网络上的正式及非正式对等网络中进行实践了。

这种方法虽然不能运用到我们期望政府做的每件事上，但是可以运用于各种特定的承诺与行动中。尽管最终结果的测量会面临很多问题（比如投入的费用及其对应成果），但随着时间的推移，我们的经验会逐渐增加，各类指标的专业知识也会逐渐丰富，这样我们就可以根据事实而非当前的各种解释来做出评估了。这不是天上掉馅饼的事——在2016年伦敦市长竞选中，就有一位候选人提出要使用区块链，来确保民选官员履行公共事务职责。[30](#)

监管部门可以将区块链流程作为一种验证方式来实时追踪所监管行业的义务履行情况，评估他们的所作所为是否如承诺所言（比如对可持续资源的投资），又是否在按照规定办事（比如及时送达、安全性目标等）。现在主要业绩指标和公共网站上公布结果变得越来越常见，不过区块链能够实现这些流程的自动执行，并确保评估结果准确无误。

这些流程生成的数据，可以让公众时刻了解到：哪个官员正直诚信？他多久参加一次例会，怎么投的投票？他有没有遵守承诺去行事？谁资助了政治运动？谁违背了智能合约条款？被选举官员及这些受监管的人，必需信守承诺，如有违背，也必需做出解释。此外，它还会给选民提供反馈，告知他们作为选民其要求是否合理、公平而不反动。选民总是希望可以多点服务，少点税；多建些工厂，但是不要建在他们的后院；又或者物价低点，工资高点等等。针对这一点，公开数据就可以让所有参与者了解到这些交易的权衡情况，从而提高他们的责任意识。

第二代民主

代议制民主很复杂，而且全球的定义各不相同，不过，有一点是不变的：被动的公民。迄今为止的讨论都是围绕区块链技术如何帮助打造平等、安全及方便的投票环境来开展的。诚然，我们有大大的机遇。基于区块链的在线投票，能够让市民给出更多的评论。但是，如果想要取代代议制民主的话是不对的。20年前唐塔普斯科特在《数字经济》中写道：“投票选项常常是对大型且复杂问题的看法总结，而这些结果产生的过程伴随着一系列冲突、矛盾与妥协。为了了解选项，负责地做出投票，市民也需要参与到上述过程中”。³¹但是，如果我们了解了新模式的轮廓，我们就会发现区块链技术所带来的帮助远不止在投票这一领域。

技术和民主：故事没那么愉快

技术是如何影响民主的呢？这个故事情节惊人地复杂。可以说，电视的出现减少了民主讨论，而前总统阿尔·戈尔所说的“思想的市场”³²也因此变成了单向对话。还有同样有毒的有线新闻电台——电视上的人通过攻击对手而不是讨论看法，来赢得收视率——而且可以看到令人目瞪口呆的极端争论。就像电影《电视台风云》里虚构的新闻播报员霍华德·比尔所说的那样：“这真是让人气疯了！我再也受不了”！

到目前为止，互联网还没有改善民主。要说有什么变化的话，那就是以国家安全为借口，变本加厉的监视以及隐私侵犯，民主政府越来越像权力主义者的政权。下面我们将集中讨论三个问题。

1. 分裂的公共言论

我们的基本制度正在遭遇诸多负面问题的侵蚀，阿尔·戈尔希望数字时代可以颠覆这一局面。“要想重建一个活跃的、众人都能参与进来的思维市场，最大的来源就是互联网。”并不是只有他一个人这么想。³³我们一直认为，鉴于网络在使用、资源及连通性方面的扩展，增加对真实信息的了解将改善公共言论的质量。

但是，事情似乎在朝相反的方向发展：对新技术的看法及研究出现了分化，在各路思想家的推波助澜下，形成了各个阵营。如今，信息的生成进一步分散，信息和观点的来源也扩散开来，任何人都可以发表某个观点并吸引同好，也许人数不多，但至少同样狂热。

新的通信方式及数据分析工具，也让那些受意识形态趋动的团体，开始“劫持”社会及政治辩论。自由派和保守派正在利用他们建立新的“回音室”，从而避免做出妥协，因此也更别提达成共识了。

2. 万维网上的无知现象正在扩张

在互联网上，人们根本无法区分一些用户是人还是狗。因此，他们

也无法总是区分出真相。阴谋论者可以在几天甚至几小时内，就散布出与事实证明相反的观点，最近的例子就是马来西亚航空MH370坠机事件。³⁴再设想一下，现在十个美国人中有三个人相信，人类从一开始就存在于世界。³⁵此外，明明有铺天盖地的科学证明二氧化碳会威胁地球生命，但是还是有人会为了短期既得利益，忽略这些证据，诋毁科学，阻断明智的讨论，并扰乱各种执行计划。网上这些传播无知与否认主义的人，正在渐渐多过科学家和理性分子。甚至有些国家正在为其市民搭建私有且受限的互联网，将网络打造成更加强有力的武器，从而打击理智的思维方式。

3.复杂的政治与实施

在数字时代之前，法律的制定与政策的实施没有那么复杂。政策专家还有总统顾问完全能够控制议题走向。不过现在，他们甚至很难时刻发现问题，更别提草拟方案或向公众做出解释了。这个问题是如此严重，以至于奥巴马总统签署了《2010年简明书写行动》法案，要求联邦机构要使用公众所理解的语言写作。³⁶

如今，竞选过程出现了很多没有预料到的问题。没有政府可以在某个事情上断言它是代表选民的意见行事的。此外，在很多问题上，政府也缺少足够的内部政策专家。因此，即使政府委托了一项民意调查，来了解公众观点，这个民调过程也不足以反映国家公民的集体智慧与洞察力。

在区块链上实现民主

这些问题都需要一个新型的民主来解决，一个重视公共言论以及公民参与度的民主。首先我们得分清，公民参与度和所谓的“直接民主”是两码事，“直接民主”是指我们通过移动设备或互动电视平台，观看晚间新闻或者对某一次公开绞刑投票。对于所有问题，公民要么就是没时

间、没兴趣，要么就是根本不懂专业知识。我们需要的是合理的看法，而非所有看法。我们仍旧需要合法集会来进行辩论、完善从而解决问题。

但是，这种合作型民主，或许也是对参与度的奖励式民主，确实能够鼓励公民参与并掌握这些问题，而且同时还能激励公共部门，在全国齐心一致的帮助下，敏锐地分析并解决问题。我们能营造出一种文化，让人们真正走上民主进程，而不是任由议员滥用职权消磨人们的积极心吗？

为什么这个想法到现在都没实现？主要原因与技术无关。大多数政治家，都更在乎选举输赢，而非解决公民参与的合法性危机。

我们从基础分析起。代议制民主最基本的流程就是选举。在民主制度下，所有合格公民都有投票权（在有些国家，比如比利时，投票也是一种责任）。然而，世界各地的选举都存在深层的漏洞。有贪官污吏擅自篡改结果，或者干脆直接操作结果。投票过程面临各种压制，从贿赂到威胁等等。操纵选举非常复杂，按时几乎各地都会发生。那么区块链技术能够改善投票过程吗？

纵观我们的技术发展，选举投票的技术几百年来几乎没有变过。在世界很多地区，选民投票得去投票站，进行身份验证，把纸质选票投入安全箱，然后再等人工计票结果。

电子投票指的是在电子系统辅助下进行的投票。在很多情况中，电子投票都被证实和人工计票一样不靠谱。现在的电子计票面临以下三个问题：软件及硬件攻击、代码错误或漏洞、人为出错。2004年，北卡罗来纳州一次普选中，就用到了投票机器，但是不小心把票池设置成了3000票，导致在竞选中无法挽回地损失了4438票，而最后决定性票数差额只是相差了2287票而已。[37](#)

区块链投票机制

那么如何在区块链上进行投票呢？设想一下，竞选委员为每个候选人或待选人创建一种数字“钱包”，经过授权的选民每选一个席位就放一个代币或其他币。公民可以通过个人化身匿名投票，只要把“币”传送到所选候选人的钱包中就可以了。区块链会记录并确认这笔交易。最后，得到币数最多的获胜。

有人尝试过结束“端对端审计投票系统”，来解决信任问题。选民通常通过自助服务终端来投票，这种方式会产生一份加密验证过的纸质记录，不过最后结果采用电子计票。

Commitcoin使用加密的工作量证明系统，来证明这一信息是在某一日期发送的。其发明者杰里米·克拉克和亚历克斯·埃塞克斯表示，我们可以利用这一系统，在大会开始前，证明选举日期的真实性。这种方法作为“碳同位素测定年代”的一种，能够为面部验证诈骗及错误提供基线。[38](#)

端对端电子投票系统

公民一直在进步。2015年，雅典大学的学者发表了一篇文章，介绍了DEMOS——一种新的端对端（E2E）电子投票系统。这种系统通过了标准模型的验证，它无须依靠设定好的假设，或接入“随机信标”[39](#)。它采用的是区块链这样的分布式公开账本，从而创建出数字投票箱，供世界各地的公民进行投票。

端对端可验证的选举设备，会监测出那些试图扰乱结果的选举当局。选民投票后，可以受到回单，让他们验证：（1）其选票已经按其意愿投出；（2）其记录结果也与意愿一致；（3）该票按记录计入最终结果。然后外部第三方会验证选举结果。不过，选民还是要接受设置好

的假定结果，并且“摒弃信仰”面对结果。[40](#)

在DEMOS的辅助下，投票系统会生成一系列随机数字。选民会得到两组数字或者密钥：一组对应他们自己，另一组对应他们支持的候选人。加密票投出后，会传送到各个服务器上。最终结果会公开发表在一个“公告板”上，并显示所有相关信息。

中立投票团体

澳大利亚有一个叫作中立投票团体（NVB）的组织，这个组织就在采用区块链选举系统，以彻底变革其民主制度。他们有一种特殊途径接近政府，并且他们的态度很乐观，他们表示：“我们相信，解决政治问题最好的办法就是亲自参与”。[41](#)

其创始人马克斯·凯将NVB描述为一款“政治软件”，通过这个软件，感兴趣的公民可以在区块链上投票，从而发表他们对政策问题的看法。时间截止后，最后计数器会指导被选官员对政府流程进行投票。当被问及为什么会用区块链时，马克斯·凯回答：“因为我们的计划是促成各方，而他们中肯定有人会强烈反对。为了保持诚信，我们需要各方都能独立验证投票记录及每一选票。”此外，马克斯·凯认为还要考虑反审查功能和不变性问题。他说：“我认为地球上只有一个电子框架能做到这一点，那就是比特币区块链。（尽管也有其他区块链，但是他们都不能做到彻底的无法篡改，因为其哈希算力指标太低了）。”[42](#)

保护选民

如果选民受到威胁，那么选举就会变得暴力。在津巴布韦，与罗伯特·穆加贝竞争的反对派在民兵对该阵营提供的武力支持导致了伤亡后，就退出了竞选。当然选举还是继续进行，最后还是罗伯特·穆加贝胜出。虽然总有人会借助技术的进步，来谋求自身利益，但也有人开始

相信，或许区块链技术能够彻底消除像亚洲这种地区的腐败问题。

在2014年7月，印度尼西亚上演了史上最具争议的一次总统竞选，一组由700名黑客组成的匿名团队，创建了一个名为Kawal Pemilu或“保护选票”的组织。其任务就是公开计算网络选举票数，从而让选民在每个投票点验证投票结果。去中心化、公开透明和个人匿名性的原则的结合，能够避免恶意网络攻击，让选举更加公平。⁴³

“腐败的政府真的想要保持清廉吗？”⁴⁴CoinPip执行总裁安森·希尔问道。CoinPip是一家专门在区块链上跨国传送法定货币的公司。他想知道是否每个人都支持投票方式的改进，政治家是否也想要更公平的选举。对其他人来说，电子投票看上去像匆忙而又不必要的跨越。我们认为，这些问题许多都属于实现范畴，而非设计问题。

我们选举与政治系统的重建，或将挖出更多民主选举投票中存在的根本问题。可以把选民身份诈骗同更阴险的事情做个比较。在2014年，美国针对选民身份诈骗进行了一次全面调查，从2000年算起，连起诉和可靠指控在内共发现31起案件，范围涉及联邦、州和市政选举。⁴⁵在当时，仅是普选和初选的投票数就超过了10亿张。

在身份认证法律最严的四个州里，超过3000张选票因缺乏适当的身份验证手段而被拒绝。⁴⁶这还不包括有意为之的人，这才是更麻烦的问题。虽然他们的民主模式领先全世界，但是大多数美国人都不投票，有人觉得“政府什么都做不好”，“政治太腐败”或者“这些选择之间没有差别”。⁴⁷希望区块链技术在这些问题方面，也能有新的解决方案。

随着时间发展、技术进步，区块链或将推动电子投票方式的革新，从而实现民主选举与民主机构的可靠转型，让选民真正有效地参与到民主进程中。

政治和司法的替代选择

如果新型区块链投票方式，能提高政府效率及反馈速度，并改善民主行政方式的话，那么它是否也能推动新的政治过程形成呢？

对于下一届政府的支持者来说，选举方式改革的最终目的，是实现一个“流动式民主”系统。投票系统公司Agora Voting的首席技术官爱德华多·罗布尔斯·埃尔薇拉也是这个说法的拥护者之一。他认为“流动式民主”是，直接民主中最完善的部分（类似古雅典实施的那种），同当代议制民主（对选民要求很低）的结合。

流动式民主，也叫“委任式民主”，这种形式的民主能够让公民最终按照个人情况与意愿，参与到民主体验中。用爱德华多·罗布尔斯·埃尔薇拉的话来说就是，在流动式民主中，“你可以在任何时间点，选择你想参与的程度。”⁴⁸你的参与会受到欢迎，但不需要你的参与来维持国家运行。

选民可以按不同话题类别将投票权委托给多个代表。⁴⁹之后根据话题分类，时不时会举办公投，然后再按话题来确定该由哪个代理（如果有选这个话题的代表的话）代替选民进行投票。在这种系统中，选民就可以选择多个可靠的专家或顾问，代表他们投票。这种理念所秉持的信念是，没有人（或党派）能够完全掌握每个问题的正确答案。在代议制民主中，这一原理常常被假定并忽略。

爱德华多·罗布尔斯·埃尔薇拉正在和政府合作，来创建“一个高度分布且独一无二的事件日志，这种日志非常擅长解决分布式的拒绝服务（DDOS）攻击。”而区块链技术就可以做到这一点。他表示：“创建一个安全且分布的系统是非常困难的，而区块链技术就可以做到.....不光因为它是分布式的，而且它还很安全。这一点很重要，对很多应用程序也很有用，比如电子投票。”其公司Agora Voting为电子选举的审计、透

明与验证，提供了一种技术基础设施。“有了一流的加密技术，在安全链中人类变成了最薄弱的环节”。⁵⁰

西班牙反紧缩措施的党派Podemos^[1]就使用了Agora Voting来进行初选。该党派承诺的参与式民主是一种透明的民主，这是在西班牙及各地发生的一种理想转变，与一种底层的分布式技术的理念是很符合的。

爱德华多·罗布尔斯·埃尔薇拉也面临一些局限性。现在为了最大化实现安全性及匿名性，用户需要整个区块链的访问权，而这是一个庞大的文件库。规模过大使得用户访问困难（尤其是对手机客户而言），这也就很难做到“用户友好型”。然而，技术在不断发展，设计也在逐渐改进。爱德华多·罗布尔斯·埃尔薇拉说：“目前电子投票还在起步阶段。”⁵¹这种技术具有柔韧性，毫无疑问，其最好的应用还有待研发。

争端解决方案

一些法律纠纷是在法院外解决的最佳案例。在商业纠纷中，智能合约能够实现去中心化的独立判决，这一点我们已经见证过了。但是，智能合约对公平或公正的概念并不关心，并且也无法去核对各种描述不一的事实版本。比起可供验证的证据记录，区块链在判决方面的革新更大，它可以作为点对点纠纷调解平台。在这种模型下，几百或者几千的与你同等的人可以组成陪审团并有效参与进来，就像Empowered Law的帕梅拉·摩根所提到的“众包式司法机制”一样。⁵²

随机抽样选举

还有一种通过区块链治理方式来实现的民主模式，那就是随机抽样选举。经过随机抽选的选民，会在邮箱收到相关方面寄出的选票及网站指导，其中网站内容包括候选人信息及相关陈述。任何人都可以申请一张（没有作用的）选票，但是它将不会纳入统计范围，而且在外界看来

跟有效的选票没有区别。人们可以将这种（没有作用的）选票卖给那些想通过购买选票操纵选举结果的人，但是对方永远不会知道这些票是否计入总数。由于这种（没有作用的）选票相比于真的选票更有可能被售出，所以这种操纵方式会产生高得离谱的费用。戴维·查姆是这一概念的提出者，他表示随机抽样投票所产生的结果，会比现在常规选举方式产生的结果，更具代表性且更加可靠。⁵³

预测市场

Augur公司就采用区块链技术，来聚集众多针对未来事件的小赌注，将其发展成更具影响力的预测模式。借助合适的应用程序，它能够帮助打造合作型民主政治。政府也能通过预测市场，让公民帮助他们了解未来情景，从而让政府制定出更合适的政策。

以太坊的维塔利克·布特因论述了一种名为由预测市场机制去驱动政策制定过程的且受欢迎的政府的政治生活替代模型。⁵⁴这一概念由经济学家罗宾·汉森构思产生，简单地说，其原则就是“投的是价值观，赌的是信仰”。公民通过两个阶段来选择各自的民主代表：第一阶段，选择一些指标，来定义国家的成功（比如文学素养或失业率）。第二阶段，通过预测市场，选择用于优化所选指标的政府政策。

Augur的预测方式可以让公民通过做出一些小的选择来参与国家的政策讨论当中，最终塑造他们所期望的民主政治的未来。

区块链司法机制

区块链也可以转变我们的司法机制。通过区块链，将透明度、众包以及在线公民参与等概念都结合到一起，我们可以设想重新将古雅典民主政治融入21世纪。⁵⁵大众司法系统网站CrowdJury⁵⁶在想办法改变司法系统，同时利用众包和区块链技术，将部分司法环节放在网络上进行操作。

作，包括控告或投诉，收集并审查证据，让公民以在线陪审团的身份，参与到在线公开审判，以及公布判决等。想象一下，这种透明化的流程会通过众包探索、众包分析以及众包决策，快速决策。这样，在更短时间里，可以花费更少资金来得到一个准确的结果。

这个流程⁵⁷可以从涉嫌公民或犯罪行为（比如涉嫌接受贿赂的公共官员）的在线报告开始，然后通过多种渠道收集信息。最初的申诉或索赔，以及证据都会通过加密，存储在区块链上，来确保其记录完整且不会被篡改。

一经立案，具备所需专业知识的小型自选志愿者团体（9~12人），会分析实情，决定这一案件是否具有审判的有效性。在审判中，需要有两个可能路径，一个是“犯事者”认罪并提出修复所造成的损害（这个是否能被接受，要看陪审团的意见），或者原告通过大汇总陪审团，来进行在线审判。正如在雅典，超过30岁的公民，在任何时候都可以申请陪审团（但不能针对特定案件），将来个人也可以通过一种随机装置，来申请决选的陪审席，就像公元前4世纪古希腊陪审员所采用的“kleroterion”投票器一样。⁵⁸因此，具体案例陪审员的分布就不会出现偏向。审判集所有证据都会在类似公开法庭的网络平台公开，任何人都可以参与，并向被告进行提问，不过只有陪审员可以通过在线投票平台对裁决进行投票。

我们可以从低价值纠纷的冲突判决开始，然后解决全球各社区的跨辖区问题，比如社交网络中的矛盾。英国民事司法委员最近就参考了全球范围内的在线模型，来推荐在线纠纷解决方案。⁵⁹大部分早期模型依赖于法官或其他专家评判员参与到这个在线过程的某些环节。其他流程依赖于其他的参与者发现并指出不良的在线行为，如诽谤性的反馈（如eBay的分支机构在荷兰市场独立反馈评论）或在某个在线游戏中作弊（如Valve's Overwatch，可以让社区的合格成员报告不良行为及在有需要的时候应用临时的禁制措施）。⁶⁰

这完全不是暴民正义。这就是“群众智慧”运用在更多司法流程中的表现，它带来了诸多有益成果。

让公民参与到重大问题的解决中

很多相信科学的人知道，人类的碳排量正在造成大气变暖。这种气候变化对我们和地球上其他生物来说是很危险的。政府、公司以及非政府组织正在努力减少碳排放，对所谓的“碳交易”他们的意见基本一致，“碳交易”是一种环境有效且经济合理的减排方案。

有一项名为“限制与交易”的政策，“限制”就是监管部门对碳排量设置一定限制，随着时间推移，减少对大气层的污染物排放；“交易”就是市场对减排的补贴，从而帮助公司及其他组织符合减排限制标准。环境保护基金会的人表示：“他们排放量越少，付的钱就越少，这样就能从经济效益上来减少污染物排放”。[61](#)

如今欧盟发达国家们已经开始了基于上述碳排放政策的交易。而加利福尼亚、安大略以及魁北克也达成了《蒙特利尔协定》，来呼吁发动全球交易。国家各级官员（包括国家、州和市）与企业层面可以通过限制与交易信贷积分制，来平衡补贴。同时，基于区块链的声誉系统，也可以根据可持续温室气体减排标准，为电网供电商进行评级。比如，系统可以为能源来源分配标签，用煤炭的会减少额度，用太阳能等可再生能源的就增加额度。区块链能够在整个行业中，实现限制与交易系统的自动化。高效的定价算法会实时计算借贷情况，然后绿色组织就能在账本上查找并追踪到其碳排放额度情况，然后将其转化成一笔交易。

那么要是我们为普通人也创建一个碳排放限制与交易系统，会怎么样呢？我们当然希望除了机构，其他人都能改变他们的行为！个人碳排放交易将会通过物联网实现。传感器、检测器以及探测仪会实时测量你

的热水器、洗碗机以及家用恒温器，并且告知你的碳排放信贷额度。同时，你也可以通过可持续的实践活动来争取信贷额度。如果你在屋顶加了一排太阳能板，那么你就能通过对电网发电来获得额度。

这种方式可以为人们创造出一个新的年收入来源吗？实际上，穷人和无家可归的人才算是低碳用户。骑车上班可以省下你家热水器可能花掉的额度：“洗碗机你好，我的个人额度与交易手表显示出我们可以负担一次整体清洁及30分钟周期烘干的操作。”。洗衣机里的水感应器可以根据可接受的颗粒浓度水平，来管理水使用情况；衣服湿度达到可接受水平时，烘干机里的湿度感应器就可以关掉烘干机；然后房子里的空调系统还可以利用多余的热量。

21世纪民主手段的运用

区块链是一种全球分布式账本，它采用可编程形式，能够保障安全与隐私，并且提供奖励机制。这项技术对新型民主工具的发展也有所帮助，比如：

数字头脑风暴：让政策官员与公民共同进行实时且适度的网上头脑风暴，来确定新的政策问题或需求。之后通过“一个代币一张选票”的系统来达成共识，并进行认真探讨。这样分裂者、煽动者还有破坏分子就很难带来伤害。

挑战赛：有一组裁判参与的在线竞赛。在区块链之前，就有类似加拿大的加拿大黄金公司创意挑战赛（第四章讨论过）、X-Prize或由西方政府组织的无数创新竞赛。这些挑战赛的目标是让公民也参与到公共价值的创新与创造中。

在线公民陪审团和陪审小组：随机挑选公民作为某类政策

的陪审员或顾问。陪审员运用网络来分享信息、提出问题、讨论问题及听取证据。区块链声誉系统可以帮助提问者了解陪审员及小组成员的背景和声誉。相关的决策和记录会登记在区块链上。

协商式民意调查：它会以合作协商的形式，为公民提供学习与反映问题的资源。这种调查将网络的小型小组讨论，同科学的随机抽样结合起来，为政策制定带去了比即时调查更多有用的公众意见。

情景规划：也就是利用仿真和建模软件搭建场景，反映未来政策制定需求，并了解决策后的长期后果。这样政治家、官员和公民就可以了解到政策对一系列领域的潜在影响，包括健康、环境以及经济等等。

预测市场：我们在Augur案例中解释过，我们有无数机会来利用预测市场，就事件结果进行买卖。政府能够通过预测市场，了解到人们对许多实质问题的见解，比如：大桥什么时候能造好？未来12月内的失业率会是多少？这些都是新西兰iPredict市场里出现的真实问题。

区块链可以为这些工具提供充足的力量。在开始时，公民中的贡献者可以保持隐私，这为参与度的提高开放了一些可能性。与此同时，上文提到的Blockapedia案例描述到，基于区块链的声誉系统可以提高讨论的质量，减少煽动者和破坏者，并确保所有评论都能准确记录且不可删除。如果需要对赢家或其他贡献者支付赔偿时，这些结算可以通过数字货币，分割成更小部分并完成实时结局。公民和团队可以创建各种各样的智能合约，从而更好地分配流程中每个人的职能。

作家梅拉妮·斯旺认为，对于一些社会话题的解决，比如统治、独立以及公民职责，区块链技术或许可以带去不断成熟的影响。“政府与经济是文化与信息的对立面，要放弃对政府与经济的中央集权似乎是比较困难的，但是我们也没有理由认为，在这种背景下就不能培养出相同的社会成熟度。”⁶²

很显然，下一代互联网会提供深刻的新机遇。主要挑战并不在于技术。有一个案例可以警告世人：2008年奥巴马竞选的时候搭建了一个大范围网络平台，MyBarackObama.com，为支持者提供了成立组织、创建社区、筹备资金的工具，诱导人们不仅仅是投票，还要参与到奥巴马的竞选中。之后出现了一股前所未有的势力：1300万支持者通过互联网联系在一起，通过自发组织，为有共同利益的人成立了3.5万个社区。当年轻人高呼着“是的！我们可以！”的时候，这不仅仅是一则希望标语了，这就是群体力量的肯定。

但是，2012年奥巴马的竞选就从公民参与转到了“大数据”。“是的，我们可以”也变成了“我们了解你”。它利用数据来争取中间选民和目标支持者的资金。最后竞选获胜，而公民却被自己的信息所利用了。大数据的策略比自发组建社区的策略风险要少很多。

在奥巴马总统的两届任期中，他确实采取了一些方式来实现公民参与，首先就是通过“竞赛”这种方式，让选民争相构思出创新想法。但是，在他关键的第二届竞选中，奥巴马却没有让公民参与进来，从而错失了一次历史机遇来加强政府的合法性。最终，就连被称作“首位网络总统”的奥巴马，也开始采用应急办法去争取权力，他利用社交媒体来传播消息，利用数据在网络上发布广告，针对目标受众筹集资金。

如果不是这位网络总统，那么会是谁？

每个人都可以将政府和民主转移到区块链上。首先，这可以提供无数机遇，包括简化繁复的过程，节省不必要的时间，投票并参与到民主过程中，担任陪审员，争取能源信用，支付税款并享受公共服务，见证税款的使用情况以及议员代表的投票过程。民选代表需要站出来，并在设计和实施智能合约的事项中展示出领导力。如果你是很正直的，那为什么不支持区块链声誉系统的创建？安德烈亚斯·安东诺普洛斯说：“选民的记性很差。”⁶³不管你是一名法官、律师、警察或国会议

员，都应该创造更多的透明度。公务员和政府雇员可以使用传感器和摄像头去在区块链上追踪公共资产和库存、管理基础设施维修的优先级，以及进行资源的分配。如果你是一个年轻人，不要放弃民主。它或许有问题，但是可以被修复的。区块链透明性的第一个用途可以是在竞选资金筹措的问题上，因为金钱政治当前是最根本的问题。如果你是一个政府的承包商，可以使用智能合约清除贪污、浪费并证明你的优秀绩效。这样的可能性还有很多。

带来改变显然是要面临很多困难的，不过世界的公民，团结起来吧！通过区块链你可以获得很多东西！

[\[1\]](#) 译者注。Podemos翻译过来就是“我们可以”。

第九章 在区块链上解放文化产业

这并不是一场平常的1岁小孩的生日派对。这个庆祝活动在伦敦一公里外的名为“Round House”的建筑物里举行。在里面的一个大棚子里，放置了能伴随声音闪烁的LED灯装饰树、充气城堡玩具以及亨利八世酒店提供的自助餐。这场活动有各种各样的参与者，包括了杂耍艺人、二十多个刚学走路的小孩及其父母、邻居、音乐家及一些区块链开发者。里面还有一个苏格兰裔印度工程师维纳伊·古普塔，他最为人所知的成果是创造了一个名为hexayurt的小型灾难舒缓避难所。现在，当要将区块链技术介绍给大众的时候，他就是所谓的“首席解释官”。另外还有保罗·帕奇菲科，他是艺术工作者联盟的首席执行官。在银行业的职业生涯结束后，他现在正为音乐家们争取权利。还有我们的主持人伊摩琴·希普，她是一个颇有成就的作曲家和音乐家，被音乐周的读者们投票选为“年度灵感艺术家”，¹她也是1岁小孩斯考特的母亲。

“我希望我正在做的事情在将来的某一天会对斯考特产生一些价值”，伊摩琴·希普告诉我们。她表达了对音乐产业的深切忧虑。“这个产业是非常碎片化的，里面的领导者很少，而且在商业的层面有很多负面的因素，”她说道。“一切事情都非常糟糕，全部是被颠倒过来的。艺术家正处于食物链的最底层。这完全是不合逻辑的。音乐无时无刻不在我们身边，在我们的手机中，在我们的出租车中，真的是无处不在。不过艺术家能获得的收入却越来越少了。”²

这就是困境所在之处。互联网是一个非凡的缪斯，它既是创意的媒体，又是言论自由的一个渠道。在互联网上，天才的艺术家、设计师和

程序员可以与他们的众多拥护者们探讨和分享一切的想法。另外，在互联网上也存在不少利用这些创意协作去实现营利的途径。像音乐这样的创意产业一直在开拓像数字作品下载、流媒体音乐等收入来源。问题是，在每一个存在中介角色的模式里，艺术家只能得到所创造收入的一部分，而且也没有什么话语权。Talking Heads乐队的名人戴维·伯恩在一个开头曲与片尾曲的作品里将这个状况概括了一下：“在我看来，作为支持任何形式的创意作品的手段，这整个模式都是不可持续的。这不仅仅是音乐。最终的结果可能会是互联网会将世界上所有的创意内容都吸走，直至什么都不剩下为止。”³

这一章的内容会关注区块链技术把艺术家放在产业模式的中心位置的方法，这样艺术家们既能享受表达的自由，又能将其知识产权所带来的精神价值和物质价值最大化。换言之，就是恢复他们的权利。不会再有庞大的、贪婪的中介机构，不再会有政府的过度干预。我们调查了文化的领域（艺术、新闻和教育），在这些领域里连最基本的人权和生计都是安危未定。

公平的音乐交易：从音乐流媒体播放到为权利定量计价

在音乐产业当前的模式下，“如果斯考特最终成为一个音乐家，她到底应该怎么赚钱？她将没法赚钱”，伊摩琴·希普在谈到她的女儿的音乐职业生涯时是这么说的。“我们需要一些简单的、核心的东西，一些可信的东西，让人们感觉音乐是一种能够谋生的职业。”⁴保罗·帕奇菲科也同意这一点：“我们希望一个能够反映出我们这个时代的文化、技术、社会及商业意义的音乐产业，并为创造者和顾客们提供一个可持续及可行的未来。”⁵伊摩琴·希普与保罗·帕奇菲科、维纳伊·古普塔及其他的一些人组建了团队，希望创造这个新的音乐生态系统。

如果有一个为创新领域而设的预测市场，我们将在希普的团队里下赌注。在2009年，她成为首个获得格莱美奖独奏作品的获得者，《椭圆曲线》是其获奖作品。她把一件“推特服装”穿在身上，从而在形式上将她所有的推特关注者都带到了颁奖典礼上。她的服装是由莫里茨·瓦尔德梅尔设计的，其特色之处是在肩膀位置设计了一个LED灯组成的拉链，可以将她的推特粉丝发出来的推文在肩膀上显示出来。在2013年，伊摩琴·希普启动了非营利组织Mi.Mu，目的是为了发明一个音乐手套系统。它将识别软件与动作传感器结合起来，这样表演者们可以用定制化的姿势来控制灯光、音乐和视频。这个发明获得了2015年的柏林奖的可穿戴IT/时尚技术奖。这个手套很快就火热起来了。流行歌手阿里安娜·格兰德在YouTube上发布了一条信息并配上了伊摩琴·希普的《捉迷藏》视频：“我想感谢我的偶像@伊摩琴·希普，她让我得以在我的首次全球巡回演出中使用Mimu手套。”⁶如果还有人怀疑伊摩琴·希普将一个社区召集起来探索新技术的能力，他们应该重新想一下。

“我们真的知道自已的需求，”伊摩琴·希普说道。“我们并不是一群喜欢在起居室制作音乐的傻瓜。我们是努力工作的企业家。”⁷伊摩琴·希普将区块链技术看成是为知识产权的创造者提供一个公平地分享价值的平台。特别是智能合约可以降低产业的复杂性，将唱片公司扮演的关键角色进行简化。

又是简单问题复杂化:音乐商业的复杂性

为了更好地理解“传声头像”乐队的想法，我们先要想明白一些问题。我们为何会处于这样的现状？我们应该如何做这件事？⁸这从艺术家们的一个基本的问题开始——他们在黑胶唱片时代遗留下来的合同模式上签约了，而这些条款适用于当时在音乐家与顾客之间存在着高昂的分销成本的年代。希普告诉我们，“当我创作了我的首个唱片时，我大约得到了15%的收入分配。我的上一张唱片是几年前的了，大约得到了

19%的收入分配。现在，如果人们运气够好，可能会得到更多的份额。”⁹艺术家们可能会将唱片著作权保护期在签约时以长期合约的形式让渡出去。在美国，这个保护期要不就是95年，或者在艺术家去世后的70年。想象一下，这样的合约若需要覆盖所有的没法预见的创新成果，而且要为艺术家和他们的继承人提供一个公平的合约，这该是多么艰难的事情。

在刚开始的时候，唱片公司是非常小的，电台就像是皇帝，录像带商店是皇后，而艺术家和节目的负责人不仅要负责寻找新的人才，还要负责其艺术发展前景。在过去的25年间，音乐产业已经从数千个唱片公司合并成三个全球的超级巨头——索尼音乐娱乐公司、Videndi的环球唱片公司以及华纳音乐集团以及几百个独立经营的唱片制作组。这三个主要的参与者一共占有了最流行、营利能力最高的流媒体音乐服务商Spotify的15%股份。¹⁰因此，如果Spotify能够在股票市场上市，它们就能获得更多的现金。苹果公司已经成了世界上最大的音乐零售商，而Live Nation则是世界上最大的在线娱乐公司。

因此，音乐的版权被掌握在少数人的手中。唱片公司和巡回推广公司已经开始与艺术家签订全方位覆盖的合约。这意味着它们可以得到艺术家创造的所有收入的一部分，从出版权到基本的作曲，到音乐录制，再到艺术家巡回演出时的表演权甚至是商家和赞助权，不管它们是否有投资到这些权利的培育过程中。

产业的合并意味着系统的整合，而这并不容易实现。每一个企业集团都有着自己的会计流程、合同版本和版税声明，这让并行对比成了一个挑战。“这个产业有一个严重的问题，它是非常碎片化的。这些不同的平台的存在可以说是一场噩梦”，伊摩琴·希普说道。¹¹这些系统必需考虑到制作、格式、分发和使用场景等领域的不同创新成果。不过，某种元素通常不会很快地过时，因此每一个环节都必需同时维护两个或以上的模式，这其中最明显的例子就是实物形式的和数字化模式的共存。

除此以外，还有一些因素会增加复杂性。产业的供应链里面成员数量是非常多的，这其中不只是出版商和演出权管理组织（管理音乐公开演出活动并收取版税的组织，如非营利的美国作曲家协会、作家与出版商协会、非营利的美国广播音乐协会以及之前名为欧洲舞台作者与作曲家协会的组织），还有制作商、工作室、各类场所、音乐巡回演出组织者和推广者、贸易商、分发商、经纪人，这些组织和群体都有着自己的合约、会计和汇报系统。他们拿走属于他们的份额并将剩下的部分分给艺术家的管理人和经纪人。最后剩下的部分才会根据他们达成的合约付给艺术家本人。没错，艺术家是最后一个拿到钱的人。根据唱片发布的时间和唱片收入会计工作的周期的不同，在第一张版税支票送达前需要等待6~18个月。

最后，一种全新的中介——像YouTube和Spotify这样的技术公司将自身插入到艺术家和唱片公司之间的供应链中，进一步摊薄了将艺术家所能分到的份额。Spotify针对每个音频流向版权所有者（通常是唱片公司）付款0.006~0.0084美元。¹²这样的支付方式初看是透明的。Spotify的网站称他们将广告和订阅收入的70%都给了版权所有者。不过我们审查了它与索尼美国公司签订的41页的“数字音频/视频分发协议”，而一些涉及对索尼的艺术家们所支付的4250万美元不可抵扣的预付款的细节则是非常模糊的。事实上，这份协议的第一段就包含保密条款。看来，Spotify和索尼都无法告知这份协议对索尼的艺术家们的收入带来的影响。美国独立音乐协会主席理奇·本洛夫称根据他的经验，唱片公司并不会分享与直接使用无关的收入。¹³“艺术家们至少还得在4~5年内忍受这个现状，就像在iTunes发布后的首个4~5年，”产业分析师马克·马利根如是说。¹⁴

那么，唱片公司到底增加了什么方面的价值？显然，他们在尝试管理这些复杂的机制、打击盗版和强化版权。例如，环球音乐出版集团让其1/3的员工在全球市场内的本地市场专门负责版税和版权管理。¹⁵环球

音乐出版集团最近部署了一个艺术家专用的通道，让他们可以分析他们的版税的状态，并可以申请以未来的收入为担保而预先提取一些钱，这个过程无须任何费用。这个通道也提供了“查看Spotify使用情况的机会：一首歌曲被在线播放了多少次，有什么类型的人在播放它，这些听歌的人的播放列表中还有什么歌曲，特定的歌曲如何与听定的听众产生共鸣。”环球音乐出版集团也安排了16个员工，专门负责这个通道的更新和为艺术家解读数据。¹⁶这些唱片公司也有庞大的律师和说客团队。他们可以在全球范围内推介新的艺术家，要求他们签订样板合同，通过外国的本地媒体进行市场推广，将他们的音乐分发到外国市场，将权利授权给外国的出版商，支持国际上的巡回演出，并将所有的收入聚合起来。管理版税的耗费已经随着业务的复杂程度增加了，这对世界各地的艺术家来说都是一个直接的负担，因为它的运作模式就像是税收一样。

区块链上的智能合约可以降低复杂性，并将唱片公司在生态系统中的关键角色进行简化。根据伊摩琴·希普所说的，“如果你是一个电脑程序、软件、数据库，这些问题就会消失了，会省下一半的时间。这些数据会直接到达目标受众，而且无须花费一到两年才能将收入分享给艺术家、作家、表演家。这个过程是即时发生的，因为它是自动化的及经过验证的。除了这些外，这种有着全新文化的音乐分发服务能够从艺术家的拥护者们收集到非常有用的数据，如果艺术家们自己能够得到这些数据，将能够让我们的效率得到极大的提高”。¹⁷这是区块链上的音乐产业的未来。

一种新型音乐商业模式的诞生

基于区块链的平台和智能合约的结合，加上艺术社区在交易谈判、隐私、安全性、尊重权利和公平交换价值等问题上的包容性、正直性和透明性的标准，可以让艺术家们和他们的协作者共同建造一个新型的音乐生态系统。

“如果我可以决定我自己的音乐的分享和体验的方式，那不是会很好吗”，伊摩琴·希普问道。“例如，可以简单地将一首音乐及其相关的内容上传到网络上的一处地方，让任何人都可以使用和获取。这些相关内容包括使用权利、所有权以及跟今天的唱片封套文字类似的说明。另外，还有视频和最近的传记”，而其他的参与方——不仅是唱片公司、音乐出版商和巡回演出推广商，还有寻找制作广告歌曲的公司、寻求制作电影原声的电视制作公司、寻求铃声的移动服务提供商以及寻求制作拥护者视频的拥护者们可以决定是否同意伊摩琴·希普的使用条款？“如果能够感受到艺术家们的存在，如果他们能够决定与自己的音乐作品相关的事项，那就会有一种非常真实的感觉，即使是每天都会有所不同。”她说道。“我可以决定，在我生日那天将所有的音乐免费送出去.....或者如果你是16岁以下或60岁以上，我来请客！或者以我的名义将所有的付款捐赠给一个救助基金，而这个过程只需要在智能合约里改动一些参数”，她说道。¹⁸

这是在区块链上建立一个以艺术家为中心模式的目标，而不是以前那种以唱片公司或技术分发商为中心的模式。艺术家们可以创作音乐并基于他们所创造的价值而得到合理的回报，至于音乐爱好者们则可以对他们所喜爱的歌曲进行消费、分享、混录和欣赏，并支付一个合理的价值。这个模式并不会排挤唱片公司或数字化分发商，但它们也会成为生态系统中平台的一员而不是像以前那样成为生态系统的主导者。

这个全新的音乐产业的想法并不是一个白日梦。在2015年十月，伊摩琴·希普通过发布了她的一首歌曲《Tiny Human》而启动了她的首个试验。所有相关的数据都能在互联网上查到：器乐版、七立体声音轨、封面图像、音乐视频、封套说明里的音乐家描述、装备、人员、歌词、鸣谢对象、有用的链接以及歌曲背后的描述。¹⁹这些细节可以增加她在互联网上的可发现性，让潜在的协作者可以找到她。

伊摩琴·希普邀请了拥护者、开发者、服务商将她的歌曲上传到各

自的平台上，并分享它的成果。她以非排他性的方式授权它们在各自的平台上创建伊摩琴·希普的艺术家档案，授权的前提是这些平台在上传希普的作品后需要把登录信息和权限分配给她。如果它们预期会产生收入，然后她就让它们提供有关支付模式、百分比和数量的信息，这样她就可以将这些细节作为她对该实验的分析的一个参考因素。最后，她欢迎大家往她的比特币账户捐款，并承诺将一半的收入直接捐给她自己的慈善机构Mycelia，这是她为这个新的生态系统取的名字。使用数据和参与行为可以为区块链的下一阶段的开发任务提供参考依据。

不同的公司正在与伊摩琴·希普和其他有远见的音乐家一起进行设计和协作。这个新的生态系统拥有一些现有的产业缺乏的特性：

价值范本：将艺术家看成是任何事业中的企业家和平等合作伙伴，并且尊重艺术家作为企业家和任何事业中的平等合作伙伴身份的协议，将他们视为价值创造不可缺少的一环。那些在一开始就埋下不平等因素的老式纸质合约应该消失了。“版税收入份额不会再下降了”，希普说道。

包容性版税：根据每个人对创意过程的贡献公平地分配收入，这不仅是对作曲家和演出家来说的，对其他的艺术家和工程师也是这样。每一个都应该在艺术品的重大成功中获得收益，而不仅仅是唱片公司和分发商。

透明账本：在区块链上的分布式透明账本让每一个人可以看到一首歌所带来的收入，收入项目的时间和大小，以及谁在带来多少百分比的收入。不会再有陈旧、私有及基于纸张的会计系统在背后记录这些事情。这个系统可以为不同性质的收入提供不同的标识（从雇佣关系的作品收入到版税收入），这能实现更简便的会计、审计和税务处理工作。

微量计费：不仅音乐可以用“流”的方式获取，连收入都可以。如

果可以微量计费的方式对音乐收费，那么消费者每次在播放音乐的时候就会支付一笔很小的费用，这样版税就可以立刻用“流”的方式支付给艺术家和贡献者。这样，付款上的延迟、半年一次或每季度一次的版税支票以及含义模糊的版税报表都会成为历史了。艺术家们也不至于继续勉强维持生计了。区块链理论家安德烈亚斯·安东诺普洛斯给出了这个例子：“阿根廷的Streamium是一个流视频服务，它让视频制作者可以为下载如200毫秒的在线流视频收取1美分的千分之一的费用。它使用了多重签名、时间锁定交易、原子性及总和完整性等技术实现这个方案。视频制作者只为消费者提供已经付款的视频，而消费者只为实际消费了的视频付费。他们的合约在每秒内自动更新五次。如果他们中的任何一方在任何时候退出，那么合约就会终止，而他们会以对双方来说最有利的交易进行结算。”²⁰

丰富的数据库：各个数据库可以在彼此之间进行互动，并将所有与核心版权相关的材料放到数字账本上，让任何人都可以看到。这些材料包括了歌词、作曲和录音，上面附带了所有的元数据、唱片封套说明、插图和照片、单曲、作曲家和演出家愿意授权的权利、授权的条款、联系信息等等，这样信息不完整的版权数据库就会成为历史了。这些版权信息都能轻易地获取。版权的所有者们可以轻松地找到这些材料。

使用数据分析：通过这个技术，艺术家们终于有机会得到与使用数据相关的分析了，这样他们可以吸引到合适的广告客户和赞助商、安排巡回演出、规划推广活动、众筹资源及与其他艺术家进行未来的创意协作。

这个模式可以捕捉到“很多在以前丢失了的数据，如你的拥护者在哪里、他们年纪多大及他们的兴趣是什么等”，希普说道，“通过这些信息，我们可以对巡回演出进行量身定制，可以与我们有共鸣的品牌和组织连接起来，或者推广我们喜欢及支持的艺术家的产品或慈善组织。我

并不是在说像姓名、电子邮箱地址这类信息，而是一些范围更小但很有用的信息。我们可以将这些数据与其他乐队的数据参考对照，这样支持者和艺术家们就可以用于很多有趣的事情上”。[21](#)

数字版权管理：这是一个管理数字版权的方式，但并非以前那种反顾客体验、只为了限制用户使用的DRM（数字版权管理）软件层。我们说的是部署智能合约，用于真正地管理版权并使得出版、录制、表演、经销和所有的其它权利最大化。这包括了为唱片公司和分发服务商而设的第三方参与的条款：唱片公司和分发商可以决定是否接受一个艺术家的使用条款和对服务的预期。如果艺术家们不希望广告行为影响音乐的体验，他们就可以禁止广告的使用。如果他们希望从广告收入中获得特定的部分，他们可以坚持这个条款。如果他们希望某个大型的公司处理授权、分发和在特定区域执行版权保护行动，他们也可以这么做。他们也可以设置条款的限制。如果公司不能达成一个具体的收入水平，那么合约可以自动被中止。艺术家们也可以在可能或有需要的情况下使用自动化的附属权管理系统，这样未来的许可证持有人可以选择接受或拒绝艺术家的使用条款和付款要求。合约自身可以执行每一项协定，而且可以在出现任何违约或中止行为时通知艺术家。

拍卖/动态定价机制：这样的实验可以用于促销和内容版本管理，甚至能够将附属权的版税的百分比与一首歌曲的需求联系起来。例如，如果消费者对某个歌曲的需求大增，那么将这首歌用于商业用途的广告客户在播放广告时所需要付出的费用将会自动增加。

声誉度系统：可以在比特币地址的交易历史和社交媒体等途径收集数据，从而为该地址创建一个声誉度积分。艺术家们将可以建立自己的声誉度，而未来的合作伙伴，不论是协作关系中的艺术家还是艺术家与消费者、唱片公司、商户、广告商、赞助商、许可证持有人等，也可以建立声誉度。通过多重签名智能合约的使用，艺术家们可以避免与低于某个声誉度标准或账户中没有足够资金的实体签订合同。

这个新型的、公平的音乐产业的关键点是艺术家处于自己生态系统的中心位置，而不是在边缘上。“我看到为Spotify和YouTube准备的位置，我看到了一个可以策展的位置，我看到一个为用户创造内容而设的位置”，伊摩琴·希普道，“我看到了唱片公司的位置，因为我们依然需要有人在全球每天新出现的海量的音乐和艺术作品中筛选出合适的内容”。²²通过软件模板，它们可以根据自己的需要在区块链上与创作者、大型唱片公司、大型分发商以及很多小型中介互动。

自我发行的艺术家：一个音乐新范式的标志

伊摩琴·希普的朋友佐伊·基廷是一个出生于加拿大的大提琴演奏家，她一直都控制着自己的音乐的相关权利。她拥有自己的录音作品的所有版权和管理权。她仔细地管理着她自己的市场推广、销售、授权和分发策略。基于上面已经提到过的复杂程度，这让我们印象深刻。“像我这样的艺术家如果没有技术的话就不可能存在了。我可以在我的地下室里录制音乐并将其发布到互联网上”，佐伊·基廷是这么告诉《卫报》的。对她来说，互联网为独立的艺术家们带来了公平竞争的机会，不过在她与大型的在线音乐分发商打交道的时候，所得到的体验跟伊摩琴·希普跟传统的唱片公司打交道时并没有显著的差异。“音乐服务商们不应该沿用过往的支付方式，也不应该利用那些处于弱势地位的人”，佐伊·基廷说道，“公司不仅对其股东有责任，也应该对这个世界和艺术家负责。”²³

佐伊·基廷指的是Google的YouTube给她的一份新合约，那份合约是不能公开的。在几年间，她在YouTube上分发她的音乐，并使用Content ID从而在第三方上传她的材料时获得经济收入。Content ID是一个能在所有权持有人的版权被可能侵害时自动发出警告的程序。佐伊·基廷并不担心隐私、文件分享和版税的问题。对她来说，商业流媒体使用是一种新的推广、吸引新听众和分析用户数据的方式。音乐内容聚合商和热门歌曲制作商通过提供满足按需服务的完整目录获得显著的收入，但

她并不包括在这之中。她的收入的绝大部分一直是来自那些忠实的拥护者为每一个新专辑所支付的20~100美元。她会先在Bandcamp上发布她的新作品，然后上传到iTunes上，最后上传到其他可以选择的地方——YouTube、Spotify和Pandora这些网站上。她使用限期策略（让内容只在一定时间内在某个特定频道的公开）已经被证明对她和她的忠实拥护者来说都是很有有效的。她可以用此回馈现有的支持者及培育新的关系。

YouTube正在发起一个新的订阅服务Music Key，在上面用户可以付费去除广告。如果佐伊·基廷希望在YouTube上继续凭借自己的作品获得收入，那么她就需要同意YouTube的条款：必需将她的完整目录包含进来，而且不能在别的平台上继续用限期策略推广作品。她要是不同意就无法在YouTube上获得收入。她知道独立的唱片制作人对这个新的许可条款也有不满，不过他们更为由此带来的经济影响感到心烦。佐伊·基廷还是希望根据她的条款去控制她的音乐。

她看到了比特币区块链技术的潜力，能够确保她的愿望能够实现，而这是从透明性开始的。“我相信透明性在任何事情中都是很重要的，如果我们不知道当前的生态系统是如何运作的，那么我们如何能够建造一个未来的生态系统？”²⁴例如，佐伊·基廷预计在YouTube网站上有1.5万个舞蹈表演、电影、电视节目、艺术项目和游戏节目的视频在没有她授权的情况下使用了她的音乐作为配音。按道理来说，她应该可以利用这些热情度，但只有YouTube知道她的音乐流行程度如何。尼尔森唱片市场调查公司是唯一的多维统计数据来源。

就如伊摩琴·希普一样，佐伊·基廷希望在区块链上注册版权并利用版权的元数据。这样，人们可以更轻易地寻找到她这个版权所有人。她也可以在区块链上追踪衍生的作品。一个储存了音乐元数据的分布式账本不仅可以追踪每个人创作的内容，还能追踪在作品中参与度较高的人。她预计可以有一个可视化的使用率和关系的监测机制，可以计算一首歌曲的真实价值以实现动态的定价，并允许向协作者和投资者发送持

续的小微付款，而无须涉及像ASCAP或BMI这样的第三方公司的“黑匣子”般的运作模式。²⁵

再重申一次，我们并不是说唱片公司和技术公司在生态系统中不再有存在的意义了，也不是说艺术家们完全可以在一个纯粹的点对点生态系统中依靠自己创造事业。我们在谈论的是一个以艺术家为中心的新型音乐生态系统，艺术家们可以在其中掌握自己的命运并为自己所创造的价值得到合理的回报。区块链技术并不会创造一个让艺术家得到补偿的新标准，而是会解放这些艺术家，让他们可以选择和定制多种符合他们需要和信仰的解决方案。他们可以将作品免费分发出去，或者以微支付的方式在任何作品上收取费用，不过在这种模式下选择权是属于他们的，而不是属于唱片公司或分发商。

新型音乐生态系统的其他元素

1. 基本的版权注册

音乐的版权有两个最基本的维度。第一个是底层作曲（用任何的形式和语言创作的音符和歌词）在世界范围内的权利，这通常是由作曲家和作词家所拥有。音乐和歌词的版权可以分开处理。作曲家和作词家可以在有人录制或演唱歌曲、购买乐谱、以另一种形式表现（如elevator Musak）、将其翻译成外国语言或将其包含到某本选集或教科书的时候收取版权费用。第二个是录音及在某种媒介（如数字文件或音乐节目录像带）上录制和保存的表演在世界范围内的权利。录制作品通常是由表演者或乐队成员签署版权许可协议，当该录制作品在电台、电视或互联网播放时，或在电视节目、广告或电子游戏上使用时，或被在线播放、下载时，或以实物媒介（如黑胶唱片、CD或DVD）的形式购买时，都会得到版权相关的收入。

佐伊·基廷那样的自主程度是多伦多工业摇滚乐队22Hertz转向区块

链寻求解决方案的动力。在加拿大，一首歌的版权注册需要花费50加元，而该证书只包含作品的标题。乐队的创始人拉尔夫·米勒并不认为若有人使用作品的歌词或旋律的话这个证书足以在法庭上发挥用途。所以，他决定使用提取哈希值（hashing）的方法，利用一个名为OP_RETURN（区块链里的一个操作代码）的功能将整首歌的哈希值上传到区块链上。如果任何人使用了他的作品歌词或音乐，他就可以利用区块链上的这个特定交易将一首歌的哈希值与在区块链上存储的哈希值进行对比，从而证明其所有权。这两个哈希值应该会是一致的。“当你将一个哈希值利用OP_RETURN操作代码上传到区块链后，经过一个个区块不断印证前面区块的记录，基本上是不可能改变任何数据了。这对我来说是非常有价值的。”当问到这个乐队的在线商店为何接受比特币支付并对比特币用户提供折扣时，拉尔夫·米勒强调，“我并不想按照往常的方式去做生意”。²⁶

2. 数字内容管理系统

Colu也希望做一些不一样的事，这是一个基于比特币区块链技术的数字内容管理平台。它为开发者和企业家提供访问和管理数字资产的工具，包括了版权、活动门票、礼品卡——这是一个分布式的音乐产业真正需要的东西。Colu与音乐技术领导者Revelator合作建造一个权利管理API（应用程序接口）。它的目标是实现伊摩琴·希普和佐伊·基廷所描绘的场景——为权利的所有权、数字式分发和实际使用带来启发。这个API也会让现有的企业有能力提供透明度及实现高效率，这两者一直有着较强烈的需求。“我们对Colu平台简化音乐版权管理的潜力感到非常兴奋，首先会从那些涉及歌曲作家及其作品的领域开始”，Revelator的创始人及首席执行官布鲁尼奥·格斯说道，“Colu让区块链的复杂技术可以整合到我们这样的平台上，而我们也期望探索所有能够为我们的客户提供更好服务的途径。”²⁷

3. 新艺术家寻找与管理

最后，人才的寻找及训练是创意产业的一个重要方面。音乐家们自然乐意在像“好声音”（The Voice）这样的竞赛节目中作为导师并扮演“新艺术家寻找与管理”的角色。区块链可通过使用率算法实现这样的“新艺术家寻找与管理”功能。我们可以看一下PeerTracks的例子，根据其网站的登录页，它是为音乐爱好者和艺术家而设的“终极的一站式音乐平台”。PeerTracks为每个艺术家上传的每一首音乐都附加一个智能合约，而该智能合约会自动地根据表演者与作词家、作曲家及乐队的其他成员所签订的协议进行收入的分配。艺术家可以创建自己的代币，上面附带了它们的名字和肖像，就像一张虚拟的棒球卡。这些代币也是一种收藏品。艺术家可以设置代币的总量。这样，就可以存在限量版的代币了。这个概念是很简单的：创造一个价值的储存方式，其价值会对应艺术家的受欢迎程度。²⁸

用户可以根据自己的需要在整个PeerTracks音乐目录上免费得到全面的访问权，而无须受到广告播放的影响。他们可以将歌曲和播放列表保存后在线下使用，并从目录中下载任何音乐或专辑。与Spotify或iTunes不同的是，用户还可以购买艺术家的代币并像棒球卡那样交易这些代币。当艺术家的受欢迎程度升高，其代币的价值也会升高，这样用户可以支持未成名的艺术家中获得潜在的经济收益。对一个艺术家的喜爱可以转化为艺术家所提供的贵宾待遇、补贴及免费赠品。这样的机制让原来在Spotify上那些被动的听众转换成活跃的推广者，并建立一个长期的、高度参与的拥护者群体。PeerTracks希望为艺术家提供更多的流媒体播放和下载的费用（具体地说是收入的95%份额）并将这些收入即时在区块链上发送出去。艺术家们可以为音乐下载和促销活动设置自己的价格。PeerTracks称“很多由利益所驱动的并寻找下一个热门明星或代币的人”将会听到一个新入行的艺术家的歌曲，因为PeerTracks的用户会投票让他们的曝光度增加。²⁹

为艺术爱好者服务的Artlery:将艺术家与老顾客连接起来

众所周知，传统的艺术市场是具有排他性和不透明性的。一群数量相对较小的艺术家和收藏家占据了市场上非常大的一部分机会，而对那些尝试进入艺术世界的新人来说，可选择的路径并不多，有时候还得经历重重曲折。即使是这样，艺术市场的开放性及整体上的缺乏规范的性质，让以下的一些尝试成为可能：试验新概念和新媒体，一方面在艺术市场进行民主化，另一方面在资产市场进行民主化，两方面都可以利用比特币区块链所带来的改革性和颠覆性的力量。

Artlery将其描述成一个由艺术家组成的网络，这些艺术家同意将其收入的一部分与老顾客及参与到他们作品之中的同行分享。³⁰Artlery的目标是在区块链上发行一个艺术品背书的货币，让艺术爱好者成为他们所参与互动的艺术品的部分所有者和股东。它的做法是为市场上的所有参与方提供合适的激励机制，这些参与方包括了艺术家、老顾客和策展人，以及像美术馆、博物馆、工作室和集市这样的场所，而不是单独地为一方保留机会而剥夺另一方的。为了让艺术家获得更多的赞助及建造声誉体系，Artlery为艺术家的作品发起了首次公开募股，用数字化的份额对应艺术家的作品。Artlery的应用程序让像姚宗·弗林斯、戴维·佩雷亚、基思·霍兰德、安塞尔姆·斯克斯塔、本顿·C·班布里奇和集市少年（the Bazaar Teens）团队这样的艺术家可以将他们的实物作品进行数字化，将作品分割成像拼图板上的一小块块拼图，然后根据Artlery的应用程序内的每一个老顾客的贡献度将这些份额分配给他们。在一个作品的IPO阶段，老顾客可以积累这些权益（最高可到艺术家在一开始时划分给社区的特定百分比）。随着平台的成熟，Artlery计划让这些积累的作品权益可以被转让和交易。

在由Artlery赞助的2015年斯坦福区块链峰会上，唐塔普斯科特决定

支持一个由安塞尔姆·斯克斯塔创作的作品，它的题目是EUR/USD 3081，是一幅放大了并被打印在一张58×44英寸的Dibond铝复合材料上的欧元纸币。

通过比特币区块链购买艺术品：如何运作

为了购买这个作品，唐塔普斯科特打开了他的比特币钱包应用程序。他使用这个软件创建了一个信息，指定了这份艺术品的购买价格作为比特币的发送数量，并将Artlery的公钥作为比特币接收地址，然后使用了他的私钥去对该信息进行“签名”（验证）。唐塔普斯科特在这个过程中再三检查了这些项目，因为在比特币系统中是不能逆转一个交易的，这跟传统的支付方法有所区别。然后，他并没有将这条信息发送到他的加拿大银行里，而是广播到由所有运行比特币完整区块链的电脑所组成的网络上。

一些人将这些电脑称为是节点，而一些节点会将它们的处理能力贡献出来以解决一个与创建区块相关的数学问题。就如我们之前解释过的那样，比特币社区将这些参与解决数学问题的节点称为“矿工”，而他们解决数学问题的过程称为“挖矿”，就像挖金矿那样。这是一个不合适的解释，因为这个比喻听起来会让你产生“专家会比普通人在这个过程中有优势”的误解，但事实并非这样。每一个矿工都在后台运行一个具备特定功能的软件，而软件负责所有的计算任务。一些专业的矿工会对他们的机器进行配置，以优化其能力及降低能源的消耗，还会使用高速的网络连接。除了这些以外，不需要人类的才智参与在其中，也不会容忍任何形式的人类干预行为。

在这个网络中，并不是所有的节点都在挖矿。实际上，比特币网络上的大部分节点只是简单地执行比特币对所接收数据的规则验证，然后将这些验证过的数据转发给点对点的连接。这个网络的验证分为两个部分，第一是证明唐塔普斯科特拥有着所指定的比特币数量并对该交易授

权，并将唐塔普斯科特的信息认可为一笔交易。然后，矿工将展开竞赛，将无序的、未被记录的交易转换为一个数据区块里有序的、记录好的交易。每一个区块必需包含其前序区块交易的摘要信息或哈希值，以及被称为nonce的随机数。为了赢得这场竞赛，一台电脑必需创建一个区块的哈希值；这个哈希值必需在开头包含特定个数的0值。至于哪个随机数会生产出满足正确数量的0值的哈希值，这在事先是无法预测的，所以各台电脑必需反复尝试不同的随机数，直到找到正确的随机数为止。这就像是中彩票大奖一样，因为这没法依赖任何技巧。不过，一个人可以通过购买最先进的计算机处理器去提高赢得大奖的概率，这样的处理器有着特殊的架构，专门适用于解决比特币的数学问题；如果用“多买几张彩票”的例子来比喻的话，那就是多运行一些处理性能高的节点；或者，就像办公室的同事们经常凑钱买彩票那样，人们也可以将他们的节点聚集起来一起计算问题（形成矿池），并同意分享其中任意节点所获得的奖励。因此，赢得奖励是与运气、处理能力及一个人所在的矿池的规模有关的。

随着整个网络所聚集的哈希速率（算力）越来越高，寻找到正确的随机数的难度也就越大。当一个矿工找到了满足含有正确数量的0值的哈希值后，就将其工作量证明（proof of work）分享给整个网络上的其他矿工。这是分布式计算领域的一项重要科技突破：使用工作量证明实现网络共识。这也被称为“拜占庭将军问题”。其他矿工通过专注于创建下一个区块的方法，将前面新创建的区块的哈希值包含到里面，从而表示他们已经承认前面新创建区块的合法性。唐塔普斯科特的公钥和私钥对他来说都是唯一的，而每一个区块的哈希值也是唯一的：它就像一个密码学的指纹一样，使得区块中的所有交易都可以被校验。不会有二个区块拥有同样的指纹信息。赢出的矿工会得到新产出的一些比特币作为奖励，这是由比特币软件自己产生并分配的，而经过哈希算法处理的区块会被添加到区块链上。

因此，在唐塔普斯科特广播了他那条信息的十分钟内，他和Artlery

都接收到了一条确认信息，表明唐塔普斯科特的比特币交易创造了被称为“未被花费的交易输出”（unspent transaction output）的项目，这意味着Artlery可以通过模仿唐塔普斯科特所做的事情就可以花费这些比特币了，那就是广播一条指定了数量及接收方地址的信息，并用Artlery的私钥授权该交易。如果艺术家和老顾客同时知道唐塔普斯科特和Artlery的公钥，那么他们就可以看到两者之间的交易被成功执行，并能看到交易所涉及的数额。这就是我们将它称为“公共账本”的原因，因为所有的交易都是透明的、匿名的，在里面我们可以看到各方的地址，但并不能看到这些地址对应的人名。每一个后续的区块都可以为之前所有交易的真实性提供确认。

下一代的艺术品老顾客档案：重新定义金钱

现在，唐塔普斯科特在一份欧元的艺术风格绘制品的相关权利中拥有了一定份额的权益。当这份实物作品卖出后，艺术家、销售场所、唐塔普斯科特及其老顾客都会根据他们的参与程度而接收到一定比例的销售所得。换言之，老顾客的参与是很重要的。若老顾客能够与艺术家及其作品互动，在社交网络上表达他们对该艺术家及其作品的热爱，激励其他人与艺术家及其作品互动，实质上为该艺术家品牌的推广做出贡献，就会得到比那些在线观看一次然后购买了权益的被动型老顾客获得更多的奖励。我们不知道在这本书中提到这份作品是否算能给唐塔普斯科特在该作品中的参与度加分。Artlery希望有一种对艺术家及其作品的积极引用的形式来表达表达欣赏度，从而与作品价值的增值相对应，这样未来的平台发布版本或许会将我们的这些例子考虑进去。Artlery在刚开始时专注于作品其中一部分的销售所得的赠与。这个平台将来会让老顾客在直接购买艺术品的所有权权益，或许能分享该作品的订阅版税收入或著作权许可所得的一部分。

通过直接地将多方（包括老顾客）引入到这个模式中，将他们作为权益持有人对待，Aetlery正在对会计投入更多的关注度。作为一个公开

的、分布式的账本，区块链确保了交易的开放性、准确性和处理的及时性。这种模式的支付范围比首次销售、二次销售以及像印刷和销售这样的附带权利更广阔，这样个体艺术家都不会再独自行动了。这些艺术家将会有有一个由持有权益的老顾客所组成的社区作为后盾，为他们商议和执行合同的权利。

Artlery用几种方式使用比特币的区块链。首先，它通过与另一个比特币初创企业ascribe.io的合作关系及API（应用程序接口）的整合将艺术作品的起源作为元数据在区块链上注册，并上传付款表，这样所有的权益持有者会立刻地根据他们的资产份额获得收入，这对所有的参与方来说都是公开透明的。它正探索使用多种将这条信息进行编码的技术，这包括了在交易中嵌入的比特币脚本。虽然它最初的目标市场是精细工艺品，但Artlery对其它如音乐、书籍和电影这样的著作权相关产业中都有着很明显的吸引力，它会通过发布自己的应用程序接口将这些市场设为目标。

将信息传递出去：教育所扮演的关键角色

比尔·盖茨、史蒂夫·乔布斯、比兹·斯通和马克·扎克伯格是广为人知的成功企业家，而他们曾经为了在数字经济时代发明一些新东西而从大学退学，伊藤穰一也是这群精英中的一员。³¹这是我们的企业家文化的一个象征，一个人若希望探索某个想法，就像伊藤穰一常说的那样“深入研究并了解其细微差别”，这就是让一个梦想家从课室走到商业里的原因。亨利·福特（福特公司创始人）和沃尔特·迪士尼（迪士尼公司创始人）在没有大学学位的情况下追逐了他们的梦想。麻省理工学院选择了伊藤穰一去管理其具有传奇色彩的媒体实验室，这是所有与数字化及文化发展相关的中心，这也是跟上面谈到的几个缺乏大学学位却走向成功的企业家相似的案例。

这个时机是非常完美的。“我加入媒体实验室之前就对数字货币很感兴趣，我在90年代的DigiCash那时候运行了早期的数字测试服务器，我所写的第一本书是用日语写的（与日本银行的某个人合著），题为《数字现金》。所以，这符合我长期的兴趣，而且很早就有关注了。”³²

在他去了媒体实验室后，一些学者还在研究与他们的主学科相关的比特币所涉及的技术，如共识机制、密码学、计算机安全性、分布式系统和经济学，但没有人专注做这些事情。他并没有看到有教员做比特币底层的研究，即使麻省理工学院的学生已经发起了MIT比特币项目，将100美元价值的比特币发放给了本科生。

伊藤穰一产生了一种像伊摩琴·希普那样的紧迫感，他希望将信息传播出去并建立与法律、技术和创造性挑战相关的团队。区块链技术的发展速度比互联网技术当年的步伐快多了，但学术界的参与程度并不多。比特币协议的核心开发者正在从声誉的打击中恢复过来：比特币基金会破产了，其董事会成员马克·卡珀利斯在日本因通过他的Mt.Gox交易所挪用客户资金被逮捕了。伊藤穰一的行动非常迅速。他在媒体实验室发起了数字货币组织（Digital Currency Initiative，简称DCI），并雇佣了前白宫顾问布赖恩·福德负责运营。他将比特币的三个核心开发者带到了DCI里，并为他们提供安稳的状态和资源，这样他们就可以专注于代码了。

他认为创建一个由对比特币感兴趣的大学所组成的学术网络是很重要的，这还在进行中。“我们正在设立课程、组织研究，不过目前还处于早期阶段”，他说道，“我们刚得到了支持该项目的核心资金，而且我们希望提高教员和学生对此项目的兴趣”。还有，他希望麻省理工学院媒体实验室重新设计更高的教育项目，这样像他这样的人就不需要退学并能意识到一个像媒体实验室这样多元化地方的价值。这是一个引领学术界的未来前进的机会。³³

作为一个处于前沿的区块链理论家和学者，梅拉妮·斯旺在让学生了解区块链这个领域的工作做得更为具体，而这并不是在传统的大学里进行的，而是在区块链上进行。“这是我们行事方式的一场翻天覆地的变革。学术机构并非实现对区块链这样的新生事物的学术思考的最佳场所”，她说道。例如，在学术期刊上出版论文需要等待18个月才能得到拒绝或出版的回复，而学者们可以像中本聪那样，将论文直接发布给有限范围的同行，实时接收评论，并建立在更大范围的受众群体中出版所需的可信性。评论者们可以像用户在Reddit论坛那样对论文进行投票。论文的获取甚至可以是免费的，但其他科学家可以向作者订阅一份深入分析或经过整理的讨论。她可以公开原始数据或其放在智能合约上并与其他科学家一起分享。如果这份论文产生了商业机会，她可与预先保护相关的权益，并考虑到为研究提供资助的机构以及它们可能对成果所主张的权利。

梅拉妮·斯旺是区块链研究学院的创始人。“这是一个教育性机构发展的开端，它的目的是支持对这些技术的学校。显然，所有的见面聚会、用户组和黑客马拉松都是非常有用的”，她说道，“每一个战略和会计咨询公司都有一个区块链实践组，还有一些像区块链大学这样的教育机构”。³⁴梅拉妮·斯旺自己在奇点大学（Singularity University）主持一个区块链工作坊的教学。

她描绘了一种教育体系，在里面一个大学学生可以成为她口中的“教育调酒师”，将兴趣或所需的技能与认可的课程结合起来，甚至可以成为大型的在线课程（MOOCs）。“MOOC是一个去中心化的教育体系，这是它的好处。这样，我可以通过Coursear在斯坦福大学参与来自Andrew Ng的顶级机器学习课程。我可以在麻省理工学院参与其他的顶级课程。”这样世界各地的学生都可以找到自己的个人发展所需的课程，并接受相应的认证。她解释道：“就如我参与GRE、GMAR或LSAT考试那样，我拿出身份证件，它在本地确认我是否本人，然后我就开始考试”，而这个本地确认“可以轻易地成为MOOC基础设施的一部分”。

梅拉妮·斯旺一直在思考如何能在区块链上实现MOOC的认证及解决学生债务的问题。区块链提供了解决这个目标的三个元素：（1）一个可信的真实性证明机制，一个用于确认申请Coursear课程的学生真的完成了该课程、进行了考试并掌握了材料的智能程序；（2）支付机制；（3）可以构建学习计划的智能合约。可以想象一个为素质教育而设的智能合约。为什么我们不将经济救援指定给个人发展用途呢？就像Kiva小额贷款项目，不过这个是为素质教育而设的，”梅拉妮·斯旺说道。除了在这里，所有的事情都是很透明的，而参与者会承担责任。捐赠者可以赞助某个儿童，将钱拨划归到学习的用途，然后根据其学习成就付款。“假如我想在肯尼亚的素质教育项目中资助学校里的一个儿童，在每个星期这个儿童都需要提供一个完成了某个阅读内容的证明。它可以通过在线测试的方式自动进行，区块链可以确认儿童的身份并记录进度，当条件满足后才会将下星期的资金发送到儿童的‘学习专用智能钱包’，这样该儿童可以在无干扰的情况下继续收到为教育任务而设的资金。一笔拨给女孩的教育费用并不会转移到她的哥哥上学的费用中”，她说道。[35](#)

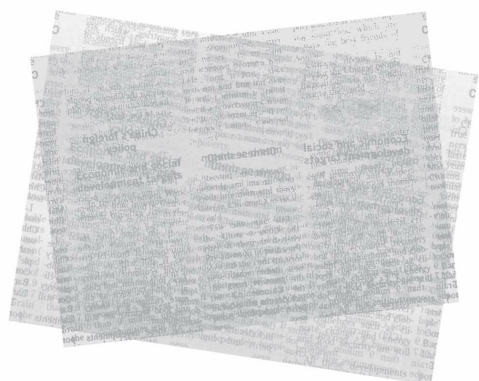
文化产业在区块链和大众的支持下成长

在一个单一的世代经历了两次世界大战，这使得全球的领导者认同政治和经济协议不能（也永远不可能）维持长久的世界和平。这些条件在改变，有时很频繁，有时还很剧烈。和平必需植根于一些更丰富、更普遍的事情中，植根于共享的道德观和社会的知识自由。在1945年，三十多个国家发起了一个教育机构，可以为和平塑造一种文化。这就是后来的联合国教科文组织。它今天在世界上的任务是“在文明、文化和人们间创造对话的条件”。[36](#)

通过区块链技术所提供的视野，它们看到了一个保护、珍惜和公平

地给予奖励的世界的轮廓。我们所有人都应该关心这个事情。我们作为一个物种，得以生存是依靠创意而不是本能。当创意产业繁荣发展，创意家们能够谋生时，我们都会受益。还有，这些是我们经济的领导者——与其他产业相对比，他们展示出这个产业内的制作者和消费者快速采用并且适应新技术的能力。音乐家们为了大众的利益的实现，一直率先探索创新的机会，而这样的成本通常是他们自己承担的。我们社会中的这些默默付出的成员给我们带来了启发，而每个商业高管、政府官员和其他机构的领袖也应该从他们之中学习数字年代的新纪元。

第三篇 机遇与隐忧



第十章

克服困难：实施过程中的**10**个挑战

列弗·谢尔盖耶维奇·泰尔曼是一个很有天赋的音乐家，不过他更倾向于物理学的研究。他出生于19世纪末20世纪初的俄国一个贵族家庭，后来加入了布尔什维克党推翻沙皇统治的运动中。他早期的任务之一是创造一个可以测量不同气体导电性及其电容量的装置。为了完成这项工作，他尝试过使用填充气体的灯泡、高频率的振荡器，甚至尝试使用催眠术去提高人们阅读仪表读数时的准确度。¹

最后，振荡器的方案工作情况很理想，因此他的老板鼓励他寻找其他方面的应用。这就产生了两个具有传奇色彩的作品。这两个作品中，其中一个是为异想天开的，它在一开始时只是两个中间没有任何东西的金属端子，就像没有气体的灯泡一样。他发现，如果他将这里的空间注入气体，他可以计量这些气体的电气性能。他的设计是非常绝妙的，他用耳机取代了仪表刻度盘，用于测量每一种气体所产生的信号的音高，这样他就可以得到听觉上的结果而不是视觉上的度数了。这种机制在当时来说是非常先进的，就像是电影《回到未来》里埃米特·布朗博士的车库里的设备一样。

Ted Talk演讲节目的忠实听众和技术历史的学生们想必已经知道这个故事的结局了：列弗·谢尔盖耶维奇·泰尔曼发现了一种用空气制作音乐的方法。当他将手放到金属端子的附近时，信号的音高就会发生改变。他意识到自己可以通过手部的精确位置和运动来控制信号的音高。他将这个设备称为etherphone，即今天的Theremin（特雷门琴，一种不需要身体接触的电子乐器），这是他的名字的英语版本。另一个应用是这个装置的大范围应用版本，可以在几米的半径范围内检测到运动。这是第一个运动探测器——名为以太哨兵（sentry of the ether）。他将这

两个设备在克里姆林宫进行展示，并在列宁面前尽情演示了他的 etherphone 设备。列宁对 etherphone 很感兴趣，然后就将这个运动探测器用于监视苏联的金库。如果任何人越过了金库附近的电磁边界，就会触发一个静音警报。这样，“老大哥”突然就装备了电子眼了。

这个故事的寓意很简单：列弗·谢尔盖耶维奇·泰尔曼的设备为世界同时带来了光明和黑暗。在一场题为“我们的电子同志”的深刻演讲中，马切伊·洛斯基指出了在列弗·谢尔盖耶维奇·泰尔曼的发明中所存在的这两个主题：当它们为世界带来了积极的因素后，很快又被滥用了。苏联政府甚至将电力作为他的宣传计划的一部分，将共产主义、苏联势力和国家的电气化联系在一起。²不过，斯大林后来将列弗·谢尔盖耶维奇·泰尔曼和他的同事抓起来并关到科雷马古拉格这个地方，强迫他们发明可以用于残酷用途的设备。

我们也听说过比特币被用于各种各样的场所，情况与上面的例子也有点相似。就如每一项革命性的技术那样，比特币区块链也有其优点和缺点。在前面的章节中，我们给你介绍了这项技术可能实现的潜力。在这一章中，我们将会关注其缺点，即可能存在的问题和风险。如果这些内容对你来说技术性太强了及太复杂了，敬请原谅。我们认为如果将这些问题简化看待的话将会是很鲁莽的行为：为了做到精确理解，我们必需处理好细节的问题。

在阅读完这个部分后，你或许会因为其所面临的显著障碍而希望将这项革命性的技术拒之门外。我们鼓励你去思考一个问题：这些障碍到底是“证明使用区块链是一个坏主意的原因”还是“技术实施过程中需要解决的障碍”。我们认为是后者，随着我们过渡到互联网的第二个时代，我们希望创新家们将这些障碍看成是需要使用创意去解决的重要问题。针对每一个挑战，我们将提出一些解决方案。在最后一章里，我们将提出一些关于如何从整体上确保区块链潜力得以实现的想法。

该技术仍未能满足大规模使用

在书写这本书的时候，大多数人只有对比特币这种加密货币的模糊理解，很少人听说过区块链技术。你们这些读者是少数有远见之人。比特币给大众的印象各不相同，有人认为是金字塔骗局，有人认为是洗钱工具，有人认为是价值传输的经济高速公路上的金融通行证。不管怎么说，这个基础设施还没到能够大规模使用的程度，这也是其存在争论的原因。

这里的挑战是来自多方面的。第一方面借鉴了科幻小说作家威廉·吉布森的看法，即未来就在此刻，而它的基础设施的分布并不均衡。即使希腊的公民在2015年希腊出现经济危机时知道比特币的存在，他们也很难在雅典城找到一个比特币交易所或比特币提款机。他们也无法将希腊的法币转换为比特币以用于对冲法币的贬值。计算机科学家尼克·绍博和信息安全专家安德烈亚斯·安东诺普洛斯都认为稳健的基础设施是非常重要的，而且它无法在危机中扎根成长。安德烈亚斯·安东诺普洛斯称希腊的区块链基础设施在那场危机中是非常缺乏的，另外由于比特币的流动性不足，即使当时希腊的法币遭遇了不少的打击，但比特币的体量也不足以让整个国家的人将法币换成比特币。

另一方面，比特币区块链自身也没成熟到让希腊使用的程度。这就是第二个方面了：如果使用率大幅度增加（假设像希腊危机需要使用比特币的情况）的时候，系统的安全性就可能会面临考验。“这个系统缺乏为1000万的人口提供服务的交易性能。这个数字意味着其用户群一夜之间会增加10倍。”安德烈亚斯·安东诺普洛斯说道。“还记得当年AOL（美国在线）在互联网上发送了230万封电子邮件的那时候吗？我们很快发现当时的互联网还没准备好，特别是在垃圾信息防护和网络礼仪方面，这不足以支撑230万没有这个文化的群体所带来的压力。这对一项未成熟的技术来说是并不是一件好事。”³区块链可能会在以下的事项上面临挑战：性能问题、系统崩溃、不可预见的漏洞，而更严重的可

能是来自对技术不熟悉的用户所产生的巨大失望——这对区块链技术的长远发展而言并不是一件好事。

上面的问题也跟比特币区块链所面对的第三个方面的困难有关，即让普通人难以使用。目前比特币区块链在钱包方面提供的支持并不多，而很多界面是对用户不友好的，使用的时候经常需要面对一些字母、数字代码和极客的技术术语。大多数比特币地址是一串从1或3数字开始、有26至35位长度的字符串，在电脑上输入非常麻烦。就像泰勒·文克莱沃斯说的那样，“你不需要输入一堆很长的字符串也能访问Google.com，也不需要输入一个IP地址。你只需要输入一个你可以记住的名字或词语。比特币地址也应当实现这样的方式，普通的用户不应该接触到比特币那种一长串的地址。这样的细微之处会有很大的影响。”⁴所以，在用户界面和用户体验方面，还有很多需要完成的工作。

批评家们也表示了对比特币长期的低流动性的担忧，因为比特币的总量是有限的，它在2140年会达到2100万的总量，而且铸币的速率是递减的。这个基于规则的货币政策目的是防止由人为或随意的货币政策所带来的通货膨胀，而这是很多国家的法币所具有的共同现象。中本聪写道，“这在贵金属上是很典型的。贵金属的供应量是业已决定的，它的价值会产生变动，而不是让供应量改变以维持价值的恒定。随着用户数量的增加，每个币的价值也会提升。这有希望成为一个正反馈循环；随着用户数量增加，价值相应地增加，这样会吸引更多的用户来利用不断增加的价值获利”。⁵

可以这么认为，存储在丢失的钱包或发送到已经丢失私钥的地址的比特币是无法被恢复的；它们一直都会在区块链上处于无人能使用的状态，因此比特币的最终流通量是要少于2100万个的。比特币的早期采用者将比特币当成是黄金储存起来，并期望它的价值在长期会有所增加，因此它们是将比特币作为一种资产而不是一个用于交换的媒介。根据经济学理论家们说的，低通胀甚至是无通胀的机制实质上是鼓励持有者把

比特币收藏起来而不是花出去。不过，如果有更多可靠的比特币交易所可以帮助顾客买卖比特币，这样交易的频率和交易量将会有所提升。如果有更多的商户接受比特币作为一种支付渠道，那么那些一直在把比特币藏起来的人或许就会开始用来购买东西，这样就能让更多的比特币流通到市面。如果商户开始发行以比特币计价的礼品卡，那么更多的人将会接触到加密货币，会更乐意用比特币进行交易。这样，理论上说，人们收藏比特币而不用来花费的理由就更少了。比特币协议的拥护者认为，由于比特币可以细分到小数点后的8位数字，如果对比特币的需求增加，那么最小的单位的购买力也能增强。另外，还有可能对协议进行进一步的修改以支持更高细分度的数字单位，这样就可以用于支持“万亿分之一比特币”的支付，也有可能在一休眠期后重新挖出一直被各种因素锁住的比特币。

第五个方面是高延时。对比特币区块链来说，交易的清算和结算需要10分钟时间，这比大多数的端对端支付机制都要快很多。不过，在销售时进行交易的即时清算并不是主要的问题，真正的问题是对物联网来说，10分钟的时间是太长了，因为物联网设备需要持续地进行互动。比特币核心开发者加文·安德烈森称为数万亿的联网设备解决问题“与比特币的设计场景并不一致，”在物联网的场景中，低延时是一个关键因素，而欺诈所带来的影响并不是很大，或参与方可以在没有比特币网络的情况下也能建立一个可以接受的信任关系。对金融交易来说，时机对“在某个价格获取某个资产”这样的操作来说是很重要的，因此10分钟的时间实在是太长了，这会给交易者带来基于时间的套利风险，如市场时机攻击。⁶对企业来说，目前可用的解决方案一直是将比特币的代码库进行分叉（复制一份），通过调整一些参数去修改源代码，并发布一个内建“替代货币”（用于代替比特币）的新区块链，作为参与网络的激励机制。莱特币是一个流行的“替代货币”，它的区块时间是2.5分钟，瑞波和以太坊都是重新设计的区块链平台，其延时是以秒计算的（而非分钟）。

第六个方面是比网络礼仪更深入的行为转变。今天，当人们出现账目错误、忘记密码、丢失钱包或支票簿的时候，很多人还是依赖于银行、信用卡公司甚至是一个人去解决这些问题。大多数有银行账户的人并不习惯将他们的钱保存到一个U盘或第二个设备中，也不会做好密码安全工作而避免依赖于服务提供商的密码重设功能，也不会将这些备份放在不同的位置以避免在一场家庭火灾中因电脑及其他物品的损失而丢失账号。如果没有这些操作纪律，他们还不如将现金塞在床垫里。区块链提供了更高层次的自由——更好的隐私保护、更强的安全性以及无须受到第三方成本结构及系统损坏的影响，但这就带来了更多的责任。对于那些无法信任自己去安全地保管私钥备份的顾客来说，第三方的存储服务提供商可以提供备份的服务。

第七个方面是社会的改变。金钱始终是一个社会概念，代表了社会所珍重的东西。它是在社会的内部成长的，它的出现是由于人际关系，而它会适应不断进化的人类需求。“你不能将金钱的社会元素剔除出去。”《金融时报》的伊莎贝拉·卡明斯卡如是说。“很多这类协议尝试通过创造一个绝对的、客观的系统而将金钱的社会元素剔除出去”，她以欧洲的体系做例子，指出一种规模和一个协议的设定并不适用于所有的国家。⁷安德烈亚斯·安东诺普洛斯认为人类需要社会原谅和忘记某些事情，社会才能继续发展下去，她也附和了这种观点。“清除系统中的记录是金融体系中一个久远的传统。社会整体认为一个人在10年或15年前做的事不应该让其在现在受到迫害或歧视。我们有这套免除债务的思维，因为我们认为任何人都应该有另一次机会。若要创建一个永远不会忘记事情的系统，那就有点反社会的成分了。”她说道。⁸

这就把我们带到了第八个方面，即在一个由不可更改的交易及不可撤销的智能合约所构成的世界中，是缺乏法律的追索权的。根据法学学者普里马韦里·德菲利皮和亚伦·赖特的说法，“人们确实可以选择自己希望接受的规则，但在决定做出后，就无法偏离这些规则，因为智能合约

会通过技术的底层代码自动执行这些规则，不管各方的意愿如何”。⁹一个交易或智能合约的结果具有高度的确定性（数学上的确定性），这在社会上是从未有过的。它带来了更高的效率，并实质上消除了违约的风险，因为无法选择违约或带来损害。不过这也有不利的一面——它缺乏为人类预留的空间。根据华盛顿和李大学法学院的乔希·费尔菲尔德所说，这意味着“它会带来更多的混乱，而不是更少。我们将可以看到更多的争议。‘你实际上并没有对我的房子进行重新装修，我希望把钱拿回来。’我们将能看到更多人为因素造成的混乱，但这并不意味着这项技术本身是不好的”。¹⁰

不过，人们真的会将对手方送到法庭上吗？普里马韦里·德菲利皮预计，在传统的世界（非数字化）里，80%的合约违约事情没有得到解决，因为上法庭的成本实在是太高了，处理起来会有很多费用。这在区块链的世界上会有所改善吗？当代码表明这个合约已经完整地执行了，并没有违约情况，但其中一方对结果不满意，他会真的用法律途径解决吗？法庭会认可这种案件吗？小商家们如果没有像大公司那样由杜威·奇塔姆·豪所组成的法律团队，那么在资源有限的情况下，他有可能识别出其匿名的对手方并提出诉讼吗？

能源消耗不可持续

在比特币区块链的这些早期阶段，第二章里描述的工作量证明机制对建立人们的信任是非常重要的。在很多年后，我们回过头来看，应该会明白这种机制的精妙之处，它解决了铸币和分配新比特币的问题，还有分配身份和防止双重支付的问题。这真是很卓越的，但根据一些对使用了工作量证明去维护网络安全和匿名性的加密货币的批评意见，这样的能源消耗是不可持续的。

用SHA-256算法对等待中的交易进行哈希运算和校验的过程需要消

耗很多的电力。区块链生态系统中的一些人对此的保守计算正成为社区里的流行话题。据估计，比特币的网络的能源耗费足以跟美国700个普通家庭的电力消耗量或者整个塞浦路斯岛消耗的电量相提并论。¹¹这超过了44.09亿千瓦时，¹²对应着很多的碳排放量，而这样的设计是刻意的。这是维护网络安全和保持节点可信性的手段。

在2015年早期，《新共和》杂志的报道表明比特币网络的总处理能力是世界上排名前500台的超级计算机累计处理能力的几百倍。“处理和保护超过30亿美元价值的流通中的比特币每年需要耗费超过1亿美元的电费，也会产生相应的碳排放量。”这篇文章的作者内森·施奈德写了一段让我们至今仍记忆犹新的话：“所有的这些计算能力，本来可以用于治疗癌症或探索宇宙，现在正被锁定在机器里面，除了处理比特币类型的交易外，什么都不做”。¹³

作为在乎我们所处的这个星球的公民，我们都应该重视这个问题。这里面有两个方面的细节，第一是关于运行机器所用的电费，第二是为这些机器提供的冷却装置（使得机器不因高温而损坏）所需的电费。这里是一个经验法则：计算机每消耗1美元的电费，它就需要50美分的电费让它冷却下来。¹⁴加利福尼亚州突发的旱灾引起了关于是否应该将宝贵的水用于数据中心和比特币挖矿工厂的冷却系统的认真讨论。

随着比特币的价值提升，挖出新的比特币的竞争也随之加剧；随着更多的计算能力投入到挖矿中，矿工需要解决的计算难题又会变得更困难。比特币网络的总计算能力是以哈希速率（hashrate）计量的。加文·安德烈森解释道：“假设在将来每个区块可以包含几百万笔交易，每一笔交易平均要付出1美元的交易费。这样，矿工们在每个区块总共能得到几百万美元的回报，而他们花费比这更少的电费去完成这项工作。这就是工作量证明的经济学的运作方式。比特币的价格及一个区块可以得到的奖励决定着全网的总算力。”¹⁵在过去两年间，比特币网络的总算力

一直在显著增加，一年内翻了近45倍。而这个趋势也会带来更多的能源消耗。

“没有中心化权力机构的代价就是能源的耗费”，一个工业级无线传感器网络公司Filament的首席执行官埃里克·詹宁斯说道¹⁶。能源的耗费就是这样的了，它可以与维护法币体系的成本相对比。“任何形式的货币都与能源有着一定的关系”，Bitpay的斯蒂芬·佩尔说道。他重新使用了黄金的比喻。“在地球上黄金是非常罕有的，因为形成黄金需要很多的能源。”黄金的高价值来源于其物理属性，而这些属性是源自于能源。斯蒂芬·佩尔认真地表示人造黄金需要使用核聚变所产生的能源。¹⁷

从一个角度来看，这些消耗的电力是有意义的。数字货币兑换服务商ShapeShift的创始人埃里克·沃里斯认为那些将花费在比特币挖矿的能源称为一种浪费行为的批评是不公平的。“这些电力是为了一个原因而消耗的，它提供了一种真实的服务，那就是维护这些支付的安全性。”他呼吁批评家们将这些花费的能源与当前的金融体系所消耗的能源相对比。可以联想一下那些大型的金库，那些配置了宏伟的希腊式建筑元素的地堡式架构，中央空调系统将冷风吹到光明的大堂，每一个街角都有互相竞争的机构分支，以及途中的自动提款机等。“下次你看到一台Brinks的运钞车时，可以将其与比特币挖矿所消耗的电力对比。哪个模式消耗的能源更多还是未知之数”，埃里克·沃里斯说道。¹⁸

第二个与能源相关的问题是计算机的自身架构。为了实现与传统系统的反向兼容性，你的笔记本电脑或台式电脑应该是一种复杂指令计算机（CISC），它可以运行范围很广的数学应用程序，而这些程序是普通人永远不会用到的。当工程师们意识到了他们给市场提供了功能过于强大的产品时，他们就创建了精简指令集计算机（RISC）。你的移动设备应该是一个升级版的RISC机器。矿工们后来意识到他们也可以使用自己的图像处理单元去增加处理速度。由于现代的图像处理单元（GPU）在每一个芯片上有几千个计算内核，它们特别适用于那些可以

并行处理的计算任务，如比特币挖矿中的哈希运算。这样的做法有得有失，而且对机器能源消耗量的估算就变得有点复杂了，不过在大部分情况下图像处理单元可以完成任务。¹⁹

“如果我可以设计一台速度超快的RISC计算机，让它可以大规模地用并行化的方式同时处理海量的代码，并只需要很少电量（或无须电量），这样我就可以凭空赚钱了”，²⁰唐塔普斯科特担任首席信息官的兄弟鲍勃·塔普斯科特（Bob Tapscott）说道。这就是比特币矿机公司BitFury所做的事：使用专门为比特币设计的节能及高效的专用集成电路（ASICs）去打造一个高度并行化的比特币相关计算专用机器。它的创始人和首席执行官瓦列里·瓦维洛夫认为机器和挖矿运作总体上会继续达到更节能的目标并对环境友好。若要实现这个目标，其中的一些任务依赖于将机器搬迁到有廉价能源（如果是水力和地热这样的可再生型能源就更好了）的气候寒冷区域，这样自然条件就能解决机器冷却的问题，或生产商可以寻找一个高效地利用热量的方法。例如，BitFury有两个数据中心，一个位于冰岛，另一个位于格鲁吉亚，还正计划在北美建立额外的数据中心。另外，它还收购了香港的一个专注于水冷技术的初创企业Allied Control。²¹通过这些途径，BitFury正致力于降低比特币基础设施对生态系统所带来的冲击。

不过，即使这些方面的尝试能够降低挖矿所带来的碳排放量，这些持续需要升级的设备的消耗量和废弃量也增长得很快。专业矿工们必需持续地升级系统并对系统进行专业化定制。大部分的挖矿设备的有效使用周期是3~6个月。²²鲍勃·塔普斯科特将BitFury这类企业比作大淘金热时加拿大育空地区的一些商店主：他们通过向矿工们售卖更好的铲子而赚钱。²³我们找到了一个矿工对其Cointerra TerraMiner IV ASIC芯片的比特币矿机的描述，称这个设备的电力消耗量太大了，他家里的电气系统完全没法承担。“我现在想卖出三个矿机，因为我的房子很旧了，电线也不合规格。我不想出现火灾。”设备的起拍价是5000美元。²⁴像澳大利

亚MRI这样的供应商正尝试一些进行回收的新方法，首先它会将这些计算元件拆解而不是简单地将它们打碎，然后根据不同的元件进行废物处理。这样的创新方法让它们可以回收贵金属并对占产品重量98%以上的元件重新使用。²⁵不幸的是，对大部分消费者来说这项硬件回收的服务并非到处都能享受到的。

对比特币的核心开发者而言，上面的担忧是合理的，而且值得去解决：“如果比特币真的成了一个全球化团队组成的网络，我想我们将需要慢慢地改变将工作量证明作为维护网络安全的唯一手段的做法”，加文·安德烈森说道，“在长期，我们将会改变一味地依赖工作量证明去维护网络的做法，而且我们将会将它与其他方式结合起来”。²⁶

这些其他的一些替代性区块链项目所做的事情：在保持去中心化的情况，探索将权益证明（proof-of-stake）这类的替代性共识算法用于维护网络安全的可行性。比特币协议的开源特性让这些工作更容易实现。要记住，共识算法意义是将区块链状态的决定权分布在一个去中心化的用户群体中。对以太坊背后的有远见者维塔利克·布特因而言，区块链上只有三类用户的群体是可以安全地实现去中心化的，而每一类用户都对应一类共识算法：运算能力的所有者对应标准的工作量证明算法；股东对应着钱包软件里的各种权益证明算法；而社交网络中的成员对应着“联盟式”的共识算法。²⁷需要注意的是，这些共识机制中只有一种是带有“运算能力”这个名词的。以太坊2.0将会建立在一个权益证明的模式之上，而瑞波是建立在联盟的模式之上——一个像SWIFT（全球安全金融信息的服务商）那样的小规模受控组织，经过授权的各个小组就区块链的状态达成共识。²⁸

这些系统不会像比特币区块链那样消耗大量的电力。Tor的创始人布拉姆·科恩介绍了第四种解决能源浪费问题的方案，他称之为“磁盘证明”，在这种机制中，磁盘空间的所有者就，即那些贡献了很多计算机存储空间去维护网络并执行网络功能的人，可以决定用户的经济参数。

针对这些工作量证明的替代方案，Blockstream的创始人对使用另类途径达成共识的方案提出了警示。“在工作量证明算法上做实验是很危险的，这是计算机科学的一个全新领域。”²⁹这给创新的工作增加了一个额外的维度：开发者们不仅需要考虑区块链的新特性和功能，还要考察哪种共识算法能够让区块链保持安全、分布性，以达到最佳的经济设定。

总的来说，“有志者事竟成”这句话是适用的。全球最聪明的技术专家们正在寻求解决能源耗费问题的创新方案，探索更高效的设备和可再生能源的使用。还有，随着计算机的智能程度越来越高，它们无疑能够提供自己的解决方案。罗杰·维尔认为，“假如最聪明的人智商IQ值能够达到200，想象一下人工智能的IQ可以达到250、500、5000甚至是500万。如果我们人类需要解决方案，总是会有有的。”³⁰

政府会扼杀或扭曲它

中本聪针对自由主义者和无政府主义者写了一段话，“你不能在密码学里找到一个政治问题的解决方案。”³¹这些人需要到别的地方寻找一个能够解决问题的万能药。中本聪将他的（比特币）实验看成是一个自由事业新领域的一个增长点，而非一个完全的剧变。政府可以成功地将类似Napster这样的中心化受控网络瓦解，而Tor这样的纯粹点对点网络将继续坚持下去。比特币区块链网络可以对抗中心化的权力机构并存活下来吗？

这或许是最大的未知之数。世界范围内的立法者、监管者和审判者将会如何对待区块链技术？“法院们已经想错了。他们已经开始想错了，将知识产权的规则应用到任何无形的东西上。他们认为物理性是虚拟财产和知识产权的分界线，但事实并非这样。”乔希·费尔菲尔德说道。“这里并不存在知识产权的因素，比特币没有一部分能归为知识产

权，这里也没有版权里的创意要素，也没有可以申请专利的想法，不存在专利，也不会有商标。”³²根据BitPay的斯蒂芬·佩尔所说，“比特币所面临的最大威胁是它越来越受到重重的监管，到了某个时候，一个更具备隐私性、匿名性的竞争者出现就可能将它的用户都抢走了”。³³有一点是肯定的：“无论特定的政策的问题是什么，如果你不理解这项技术及其影响，你就注定要失败了”。比特币政策智库Coin Center的杰里·布里托说道，“如果你不理解它，你就可能会引入一些对这项技术的发展带来伤害的法律和政策。我只是想你去理解我们在做的事情”。³⁴

这些挑战是非常巨大的。他们必需预见所有意外的情况。另一方面，他们必需避免对那些反面例子产生非理性的反应，否则就可能扼杀创新。这些反面的例子包括人口贩卖、非法药物交易、枪支贩卖、儿童色情、恐怖主义、逃税和造假等。还有，他们也不应该将尚未经过实践证明的应用程序（如与区块链的身份管理平台）的用途扭曲并用于限制公民权利。另外，必需有一些稳定的途径去处理监管、立法、国际协商条约等事项，以让监管不确定性问题最小化，这样投资者们将继续支持这项技术的全球发展。

在使用比特币的时候，处于哪个辖区已经是一个重要的问题。一些政府已经禁止比特币的使用，或禁止国有银行交换比特币。杰里·布里托说道，“这么做并不是非法的，但或许在任何时候就被称为非法了，每一个人都知道这个状态”。³⁵政府容许了一些大型的专业挖矿社区的发展，这些矿池现在已经在是否对比特币协议进行升级的争议中具有非常大的影响力。如果政府突然禁止了比特币挖矿，那么比特币的安全性会面临什么问题？其他辖区对比特币的性质进行了更严谨的定义，就如美国国税局所做的那样。美国国税局将比特币作为一种资产看待，认为应当在增值时进行税务的计算。

法律框架也是很重要的。法律学者普里马韦里·德菲利皮和亚伦·赖特并不认为当前的法律框架可以解决智能资产在全球内部署的问题。智

能合约会定义和管理所有权。它们的代码对权利的分配并不会做出假设，而代码也不能随意地冻结、剥夺或转让这些权利。例如，如果在土地登记的过程中，政府官员将一宗土地的所有权分配给一个并非该土地合法所有者的人，那个人将可以对该土地主张权利，而合法的所有者将无法逆转该分配。

乔希·费尔菲尔德对过程更为关注：“普通法并没有对技术法产生影响。普通法就是技术法。普通法正在适应人类系统的技术性改变的过程。真正的挑战来自我们如何将旧技术而设的旧规则快速地、可靠地应用到新技术上”。这样的话，当我们使用它的时候就可以得到承认，其可迭代性让它可以保持最先进的状态，当技术真的得以应用的时候就能做好准备了。[36](#)

最后，身份是很重要的，这并不应该令人感到惊讶——最起码我们在区块链上构造身份的方式是很重要的。“人们对身份看得太简单了”，安德烈亚斯·安东诺普洛斯说道，“我实际上很害怕数字身份带来的影响，因为我认为人们会走捷径，如果我们将身份转移到一个不具备灵活观点的数字世界中，我们最后可能不会得到一个跟身份的社会架构相关的结果，而是一个可怕的法西斯版本”。[37](#)

如果将人格的精确代码版本与社会的精确代码版本结合起来，你就可能会得到科幻小说及施瓦辛格的电影里描述的东西。法律学者普里马韦里·德菲利皮和亚伦·赖特描述了如下的场景：“自我执行的合约，安全的系统或可信的系统，由去中心化机构组成的复杂网络持有和管理，这个网络决定了人们可以做、不可以做的事情，没有任何形式的宪法保护和限制”。换言之，一个由机器驱动的极权主义体制。

人工智能专家史蒂夫·奥莫亨德罗将这个阶段看成是独裁者的学习曲线，或洞穴人是如何得到航天年代的科技的。想一下，世界上的人工智能实验室里有很多世界上最聪明的博士，配有世界上最强大的计算

机。这些博士或许会分叉（复制）比特币的代码或写一个可以控制无人机运送包裹的智能合约，在这里面当包裹送达后存放在托管账号里的比特币才会支付出去。我们假设一下，若这些博士在互联网上用开源的形式发布了这个软件，因为这是他们验证并追求想法的一种做法，他们分享主意。这样，ISIS并不需要人工智能实验室，它只需要将这个包裹里的货物替换成手榴弹。这就是独裁者的学习曲线，而且难度并不大。但是，不要将这怪罪于代码或分享的文化。这并不必然是与我们使用代码的方式有关；而是我们并不知道在使用它所做的事情，这就是一个没有摩擦的世界所存在的不可预见的后果。

旧范式的强大既得利益者会介入

我们对第一代的互联网所产生过的很多担忧已经成为现实。大型公司已经获得了大部分的技术并将这些技术用于其私人帝国，从而获取了大部分的价值。他们已经将机会封闭起来，并将我们绝大部分的数字化体验私有化了。我们现在要依赖于专有的在线商店以在我们的手机、平板设备及手表上获取和使用新的应用程序。搜索引擎和市场营销部门通过广告干扰我们对内容的体验。众所周知，那些推行并从顾客信息的透明性中走向成功的大公司对它们的活动、计划、技术基础设施和信息资产一直保密。当然了，一些公司已经主动将这些公开了，但很多的其他公司仅仅对知情者和调查报道做出回应。这样的信息公开程度是被隐藏运作流程和信息的活动矮化了。

简而言之，它们一直没有成为公众信任的可靠服务员。

银行产业是一个恰当的例子。“银行传统上就是秘密保管者”，《金融时报》记者伊莎贝拉·卡明斯卡说道。她解释道，银行若能得到很详尽的私人信息，就能更好地决定向哪些人发放贷款以及如何处理付款，而银行之所以得到这些信息是因为它们做出了会保管好这些秘密的保

证。银行掌管秘密越多，信息不对称的程度也随之增加，这样银行就能占有优势。不过，这样的优势带来了不良的系统性影响。³⁸所以，有什么事情能组织大公司或强大的国家将区块链技术用于他们狭隘利益的实现呢？“任何共识机制都可能受到市场营销的影响，因为强大的利益集团会尝试花钱去说服人们做某件事情。”BitPay的佩尔说道。³⁹

这里要澄清一下，我们并不是让公司和政府远离这个技术。毕竟，区块链技术已经呈现出了作为一种重要的全球资源并实现提供新能力的潜力。还有，社会需要政府为其公民服务，也需要公司去创造工作职位和财富，但这与限制其对社会更大益处的方式夺取这项颠覆性技术及其潜力是不一样的。

另外，也可以考虑核心开发者和比特币相关公司所做的与网络安全性有关的事情，对最坏的情况进行预测并做出反应。例如，在2014年，黑客从Mintpal交易所盗取了800万的Vericoin（一种权益证明的加密货币）。在攻击发生后的几天内，Vericoin的开发者发布了一个对攻击发生之前的Vericoin区块链进行分叉的新代码，这可以看成是回滚到过去的时间，并与交易所一起确保这个新的版本被采用。⁴⁰类似的情况还有，“如果资本家和权力真的希望夺取这个网络，矿工们可以通过跑到比特币真实版本并开始一个分叉的方式阻止他们。”⁴¹Blockchain公司的产品主导人员纪昂·罗德里格斯说道。

有什么措施能够防止有些国家将政府的计算机处理能力和所有的矿池对比特币区块链进行51%攻击或最至少降低比特币运行的稳定性？假设有一个富有的强权者认为比特币会像之前的互联网一样削弱他的权力。这个强权者将会冻结所有能够接触到的挖矿能力并从国内还能容忍他的不良行为的人群手里购买剩余的挖矿设备，从而让自己拥有超过51%的算力。到那时候，他就可以决定区块可以包含或拒绝哪些交易。在占有了控股权益后，他就可以决定是否对代码进行分叉并引入一些新的禁令，或者是将一些与赌博或其他相关的地址放到黑名单。那么，诚

实的节点应该采用这个中心化控制的分叉版本，还是应该分叉到一个新的代码中？莱特币协会主席安德鲁·维基特比尔称在这种情况下并没有解决方案，因为强权者这时候已经控制了51%的网络算力。而且，他也不需要是来自一个政府的代表；他可以是世界上那群最富有的人中的一员，或者是一个营利能力极强的公司的高管（拥有强大的购买力）。[42](#)

第三种情况是现有的参与者会捍卫它们的领土，并参与游说活动，以确保为大型公司制定的现有监管体系应用到小型的初创企业上，并起诉任何能够从监管干预中存活下来的初创企业。这个“起诉而不创新”的策略可能会为他们制定新战略争取一定的时间。或者，这个策略会让现有的参与者逐步走向衰亡。想象一下这对暴君双胞胎——陈旧的系统 and 刻意的惰性。学术界已经仔细记录了历史成本及切换系统的成本，并发现了一些与合并后系统整合工作相关的挑战。那些在它们现有的系统投入了很多技术投资的机构更可能在现有的老式系统上花钱，就像将它们的刀子磨利并用于一场枪支决斗那么滑稽，而不是在区块链上进行战略性的实验。

对分布式大型协作的激励并不充足

矿工们确实有维护比特币基础设施的动力，因为通过挖矿所赚到（或有可能赚到）的未售出的比特币将会丢失或一文不值，或至少会存在风险。在我们深入研究激励机制之前，我们先明确一下矿工提供的服务：它所提供的并不是交易确认服务。每一个完全节点可以进行交易的确认。不过，矿工们保持了权力的分布——决定哪些交易可以被包含到每一个区块链的权力、铸币的权力以及就事实进行投票的权力。

所以，你想成为一个比特币矿工吗？

作为我们研究的一部分，我们在2015年早期雇佣了银行前首席信息官鲍勃·塔普斯科特（他现在是知名的管理顾问）以及唐塔普斯科特的兄弟去下载整个比特币区块链的数据堆栈及账本。这个实验的运行时间、所需的工作、消耗的能源以及对比特币的业余矿工报酬（或没有报酬）的状况相当有启发性。

鲍勃将他闲置的双核四线程Windows台式电脑投入到这个任务中。下载的过程使用了整整三天时间，平均消耗了20%的可用处理能力。挖矿使用了比200MB多一点的内存，以及10%的CPU资源，以维持最新的状态。

虽然鲍勃的电脑并没有为比特币挖矿进行优化，不过他将这台电脑投入了一个矿池中。在一个137小时的时间段，它挖出了152.8uBTC，在当时大约价值3.5美分。不过，以10美分/千瓦时的费用计算的话，Bob的电脑使用了大约价值14美分的电力。Bob的结论是，“从你的个人电脑上进行比特币挖矿的日子已经结束了。”

因此，对原始的比特币协作做出的任何更改（不管是通过替代性货币还是一个升级过程），必需要考到为矿工提供合适的经济激励以维持矿工的去中心化，这样网络就可以通过大量的比特币去换取矿工们所提供的良好贡献。比特币核心开发者彼得·托德将这个任务与设计一个能在杂物店买牛奶的机器人联系起来。“如果这个机器人没有鼻子，商店主人很快就能意识到它不能分辨正常和变质牛奶的区别，那样你就可能会为一堆变质的牛奶付费了。”⁴³对托德来说，这意味着在地理上分散的小型矿工应该可以与地理上集中的大型矿池（冰岛或中国的）相竞争。

问题是，这是否可能实现。由于比特币的新产出量每四年会减半，当奖励降到零的时候会发生什么事情？挖矿的流程依赖于比特币的市场价格。当价格下降，一些比特币矿工就会暂停他们的供应，但他们还是会继续碰运气并等待价格的回升。其他矿工无法承担暂停供应和赌运气的风险；他们会拆除挖矿设备或将算力投入到其他更有利可图的区块链项目上。这样，其他人还是会加入矿池，希望他们的算力加起来至少能增加赢得一部分奖励（而不是什么都

没有)的概率。这就是比特币挖矿产业的现状。BitFury的瓦列里·瓦维洛夫预计他的挖矿业务在2016年末期将至少有2亿瓦特的容量。

另一个方法是收取费用。中本聪写道,“始终会有交易费用的,这样挖矿节点还是有动力去接收交易并包含到区块里。当产出的比特币总数达到了预先设定的限制时,节点最终依靠交易费用就能得到补偿了”。⁴⁴所以,当比特币被全部挖出后,就可能会出现一种新的费用架构。想象一下数十亿笔的微型付款,由于每一个区块有固定的最大尺寸,就会有一个矿工可以包含进去的交易数量的限制。因此,矿工们会先将费用最高的交易添加进去,然后让那些低费用或零费用的交易竞争剩下的区块空间。如果你的交易费用足够高,你可以预期会有矿工包含到下一个区块里;但如果网络处于繁忙的状态而你的交易费设置得很低,那么就可能需要2个、3个或更多的区块才能最终被一个矿工添加到区块链里。

这对那些无法承担交易费的人来说意味着什么?区块链相对于传统支付方式的优势之一不是低廉的费用吗?根据风投家帕斯卡尔·布维尔所说的,“交易费反映了交易验证的边际成本”。如果缺乏用于激励矿工的交易所,随着区块奖励不断减半,网络算力更可能随之下降。如果网络算力下降了,网络的安全性也会降低。⁴⁵

这又让我们回到了51%攻击的问题上,即当一个大型的矿池或矿池联盟控制了51%的全网算力的情况。有了这么多的力量,他们就可以占据大多数的矿工投票权,可以劫持区块的生成并将他们自己版本的事实强加到比特币区块链上。他们不一定会变得很富有,远非如此。他们可以做的事情只是逆转与自己有关的历史交易,就如信用卡的退款交易一样。假设攻击者从同一个商户里购买了一些大件商品,等货物运到后就对网络进行攻击并拿回他们所付出的钱。这并不意味着将自己的区块附加到区块链的末尾位置上,而是即使在网络持续产出新区块的时候,回到历史交易上并重新构造包含他们购买交易所在区块及所有相关区块的记录。当这个攻击者联盟的区块链分支的长度更长时,就会成为新的有效分支。中本聪认为这样的攻击比挖出新币的成本更高。

工作量证明模式的51%攻击来源于集中的挖矿算力，而权益证明模式的攻击来源于集中化的代币控制，而代币交易所通常是最大的权益持有者。在一些辖区，交易所必需取得牌照并接受监管。这些交易所需要维护其声誉，这样它们有多个层次的动力去保护它们的品牌价值以及在账户钱包里的代币的价值。不过，随着代币的流通量增加，价值的分散程度越高，还有更多战略性的资产登记在工作量证明和权益证明区块链上，攻击者或许不会在意这些成本。

区块链会对就业带来冲击

在2015年瑞士达沃斯世界经济论坛里，来自微软、Facebook和Vodafone的技术高管所组成的小组讨论了技术对就业带来的影响。所有人都同意技术创新或许会对劳动力市场带来暂时的冲击，总体上说它们能创造新的职位和更多的职位。“这次为什么会有所不同呢？”Google执行主席埃里克·施密特说道。

自动化对工人的取代并不是什么新闻了。你可以考虑一下互联网对旅游中介和音乐零售商带来的影响。Uber和Airbnb为有着闲余时间的司机和有着空闲房间的房主创造了收入，但它们都没有提供医疗保险或其他雇员福利。它们还在旅游和招待产业不断取代收入更高的工作。

区块链是一个极佳的自动化平台，它由计算机代码而不是人类活动去执行工作、管理资产和人。当无人驾驶汽车代替Uber司机时会怎样？或者当数字货币取代了西联汇款的50万个办公室时会怎样？⁴⁶或者当一个共享的区块链金融服务平台取代了成千上万的会计和IT系统管理工资时会怎样？物联网当前正创造了很多新的商业和雇佣机会，但它将来会导致一些相对来说无须技能的市场（如一些相对例行的任务）的失业率增加吗？

在发展中国家，区块链和加密货币可以让企业家募集资金、保护资

产和知识产权，甚至能在最穷的社区创造工作职位。数亿的人可以成为新公司的微小股东并参与到经济交换中。这些技术可以极大地改善救援资源的分发和部署，提高政府的透明性，减少腐败现象，并为良好运作的政府设定标准——在世界各地这是创造职位的先决条件。

即使在发达国家，这项技术的影响也未有定论。一个能够降低交易成本（特别是建立商业信任关系和财富的成本）的全球平台可以吸引更多的参与者。

即使这项技术让我们用更少的人力资源就能实现完成更多的工资，我们还是不需要担心、推迟或暂停它的到来。最终，关键的问题并不是这些新的潜力是否存在，而是社会应当如何将这些技术为社会带来价值。如果机器最终可以创造很多的财富，到那时候可能就需要一个新的社会契约，重新定义人类的任务及谋取生计所需花费的时间。

协议的治理就像是牧放一群猫

我们应当如何推动这项技术实现其潜力？与互联网不同的是，比特币社区仍未有建立类似ICANN、互联网工程任务组或万维网联盟这样的正式监督机构，以预期发展需求和引导议程，但比特币社区更倾向于没有引导力量的方式。这带来了不确定性。那些希望保持区块链的去中心化、开放性和安全性的人无法就前进的方向达成一致。如果我们不重视治理机制，这样区块链就会因令人担忧的派系斗争而自己瓦解。

这里面有数不清的问题。比特币核心开发者加文·安德烈森和迈克·赫恩一直推动将区块尺寸从1MB提升到2MB上限的提议。“比特币不是一个有钱人用于反复交易的代币，而是一个支付网络。”加文·安德烈森说道。⁴⁷他们认为如果比特币希望作为一个全球化的支付体系参与竞争，那么就必需为主流的应用准备好。它不能在交易量突然超过区块链

容量的时候慢慢瘫痪下来，否则对那些不希望等几个月或几年才能结算交易的人来说交易费用就会变得很昂贵。或者，某个中心化的力量会介入，以保护消费者的名义处理这些过多的交易量。在2015年8月，他们直接发起了Bitcoin XT，这是一个允许比特币区块链处理8MB区块的分叉版本。不过，这还是一个具有争议性的妥协方案。

反对的声音认为人们不应该用比特币在星巴克买超大杯的拿铁咖啡。“一些开发者希望世界的每一个人可以运行一个完全的校验节点，可以看到每一笔交易，而且不会信任其他人”，加文·安德烈森说道，“那些在过去几年间一直在开发这个软件分叉版本的志愿者们担心自己在交易量突然提升时无法处理更大的区块。我对那种情况并不表示同情”。⁴⁸换句话说，如果比特币区块链希望扩展容量及保持安全性，我们就无法二者得兼。一些节点将会运行完全的协议并将更多的交易处理成逐渐增大的区块，而其他节点将会运行简化的支付校验模式并信任51%以上的完全节点能够正确处理记录。

Bitcoin XT最大的阻力来自中国的矿池。那些专业的矿工（与专业在线游戏玩家有相似之处）不仅需要强大的计算机去找到一个正确的哈希值，也需要高速的网络带宽以将其在网络上快速广播出去。中国并不符合尼尔森的互联网带宽法则（Nielsen's Law）所描述的情况：网络带宽并不会以每年50%的速度增加。如果区块尺寸增加得太多，那就会让低带宽的中国矿工在与世界其他地方的矿工相比之下处于劣势——收到一个构造下一个区块所需的新区块将会花费更长的时间；当中国矿工真的找到了一个新区块时，他们需要花费更长的时间才能将它发送到网络中的其他部分。这样的延迟最终会导致网络拒绝他们所产出的一些区块。这样，他们就会在输给拥有更多带宽的矿工，因为他们的区块可以传播的更快。

“尝试去引导或改变一个网络协议实在是一个巨大的任务”，奥斯汀·希尔说道。“你不希望在一个管理着10至100亿美元价值的财富和资产

的生态系统里做出临时或频繁的改变。”⁴⁹加文·安德烈森说道，最终“治理的模式主要是由人们实际想运行的代码版本而决定的，由那些人们在它们所出售设备上所整合的标准决定的”。他认为比特币就如互联网一样，“会有一种类似的混乱情况，无秩序的治理过程最终会取决于人们选择运行哪一份代码”。⁵⁰

再次重申，我们并不是在讨论“监管”的问题，而是管理其生存和成功所需要的资源。治理（**governance**）包括了设定标准、提倡并采用明智的政策、发展与该技术潜力有关的知识、执行监督功能并真正得建立一个全球基础设施。我们将会在下一章讨论一种由多个权益所有者参与的治理模式。

自主运作的代理人会形成“天网机器人”

世界上存在一些具有高度分布性的企业，其中的参与者各有好坏。**Anonymous**是一个分布式的、由志愿者组成的紧密团体，它的成员包括公司破坏者、检举者以及监督者。通过区块链，**Anonymous**可以使用比特币进行众包并将这些资金放到一个钱包里。假设有个由法国股东组成的小组希望采取措施以追踪和消灭那些对巴黎大屠杀负有责任而尚未落网的恐怖分子。他们需要几千个（密码）签名才能达成共识并释放资金。在这种情况下，谁是这些资金的合法控制者？谁要为这个交易的结果负责？如果你贡献了一个投票中的万分之一份额，你在法律上有责任吗？⁵¹

如果自动售货机的程序是“订购利润最高的产品”，它们会找到一个非法商品或药物的供应商吗？（想一下，糖果售卖机在卖非法药物！）法律应该如何处理无人汽车意外地导致人类死亡的情况？据《**Wired**》杂志报道，两个黑客展示了如何劫持一辆在高速公路上的吉普·切诺基

（Jeep Cherokee）汽车的控制系统。克莱斯勒公司对此做出了响应并召回140万辆汽车并对司机、生产商和政策制定者发出了警示。⁵²恐怖分子能找到入侵智能设备的方法从而让它们执行有着灾难性后果的任务吗？

企业的分布式模式面临着其他的挑战。社会应该如何实施对这些实体的管理？所有者如何保持终极的控制权？如何防止对无人运行业务的敌意控制？假设我们拥有一个去中心化的网页托管公司，每一个服务器对公司管理都有发言权。一个人类黑客或恶意软件可以假装是100万台服务器并超过网络中的合法服务器的票数。当传统公司发生这种并购的情况时，结果可能有很多种。而在分布式的自主运作企业里，这样的结果可能就是灾难性的。当这个恶意的实体控制了我们的分布式网页托管公司，它可以把里面的资金都转走。或者，它可以把其他服务器的隐私数据都公布出去，或者劫持这些数据直到我们这些人类所有者支付赎金为止。

当机器拥有了智能和学习的能力时，它们进化为自主运作的速度有多快？例如，军用无人机和机器人会决定对付平民吗？根据人工智能领域的研究人员的说法，我们离这种武器的实现只有几年了（而不是几十年）。在2015年7月，一个由科学家和研究人员组成的大型组织，其成员包括斯蒂芬·霍金、埃隆·马斯克和史蒂夫·沃兹尼亚克，发布了一份公开信，呼吁禁止发展任何超出人类控制范围的自主运作的进攻性武器。⁵³

“对我来说，一个噩梦般的新闻标题是《10万台电冰箱攻击了美国银行》。”文斯·瑟夫说道，他被广泛地认为是互联网之父。“这不仅需要认真考虑基本的安全和隐私保护技术，还要考虑如何在大范围内配置和升级设备。”他补充道。他注意到没有人希望浪费整个周末的时间为每一个家庭设备设置IP地址。⁵⁴

我们并不建议对分布式自主运作企业和物联网实施广泛的监管或监管审批的机制。我们会建议那些正在开发应用程序的企业家识别任何对公共利益带来显著影响的因素（无论是好的，坏的，还是中性的），并修改源代码及其设计方案。我们认为他们应当咨询那些可能会被这些发明所影响的人，以提前将风险最小化、寻找其他解决方案和构造支持体系。

老大哥还在监视着你

“将会有很多人希望控制这个网络”，Blockchain公司的纪昂·罗德里格斯说道，“大公司和政府将会致力于打破隐私保护”。美国国家安全局必然已经在积极地对区块链数据展开分析⁵⁵。虽然区块链确保了一定程度的匿名性，但它也提供了一定程度的开放性。有史为鉴，我们应该预期那些有着间谍行为的公司及展开网络战的国家会将它们的行动升级，因为这涉及了价值——金钱、专利以及对矿产所有权、土地所有权及国家的财富的控制。这就像是在互联网上放了一个巨大的靶心一样。不过，有个好消息是任何人都可以看到这些恶作剧。一些人可能会很有动力曝光那些间谍行为，因为他们会在一个预测市场上对某个特定机构攻击区块链的可能性下注。

当物理世界开始收集、通信和分析可用于持续追踪个人信息的无线数据时，对隐私保护意味着什么？在2014年的Webstock演讲中，马切伊·洛斯基指责了Google对Nest的并购案例。Nest是一个豪华型恒温控制器的制造商，这种控制器配置了可以用于收集房间数据的传感器。他的旧恒温控制器并不涉及隐私保护的问题。这个智能的恒温控制器可以向Google汇报信息，甚至可能像一个可疑的室友那样吃掉他剩下的比萨饼。⁵⁶我们之中的很多人已经对社交媒体环境能够追踪我们动向及到处向我们展示个性化的市场营销信息的现状感到不安。在区块链的世界

里，我们将会对这些事情有着更好的控制，但我们将能有足够的警惕性去管理我们的媒体大餐吗？

这些隐私的挑战都不是真正的障碍。马切伊·洛斯基继续说道：“好消息是，这是一个设计问题！我们可以搭建一个分布式的互联网，它有着强大的生命力以抵御不同的干预，并让世界变得更好”，就如我们在20世纪90年代对它的期望一样。隐私和大数据学院的安·卡沃基安概括了7个“对商业、政府和公众”有利的原则。将隐私保护作为默认的设定是关键。拒绝那些将安全性与安全性相对抗的错误两分法；每一个IT系统、每一个商业实践及所有的基础设施都应该有全面的功能性；领导者们需要提前预防而不是在事后应对入侵行为，在所有的运作过程中保持透明性，并让自己的组织接受第三方的检验。通过尊重用户的隐私、将用户放在设计的中心点考虑问题、确保端对端的用户数据安全及销毁不再需要的数据，企业（及其品牌）将会得到人们的信任。她说道，“这真的是一个双赢的提议，拒绝零和游戏并拥抱正和的关系”。[57](#)

马切伊·洛斯基说道，“不过这需要投入很多的工作和决心。它意味着推翻那种将长期大规模监视当成是商业模式的做法，这会产生阵痛。这也意味着在一个僵化的法律系统里推行法律。争议也是会有的。不过如果我们不设计这样的互联网，如果我们继续在现有的模式上建造下去，那么新的模式最终会吸引到一些卓越的、有远见的人。到时候我们或许不会喜欢这些人的存在，但到时候我们的想法已经没有意义了”。[58](#)

罪犯们也会使用这个网络

在比特币发展的早期，批评者们经常将比特币看成是洗钱或购买非法商品的工具。批评者们认为因为该技术是去中心化、高速及点对点运作的，罪犯们会利用它。你很有可能听说过“丝绸之路网站”，这是一个为非法药物而设的地下网络市场。在2013年10月，丝绸之路最高曾经有

13756个商品是以比特币定价的。上面的产品通常是以邮件运送，还附带了避免被当局检测到的指引。当美国联邦调查局查封了该网站后，比特币的价格出现暴跌，数字货币也成犯罪的代名词。那是比特币最黑暗的日子。

不过，与其他技术相比，比特币或区块链技术对犯罪分子所提供的便利其实也没有什么独特之处。有关的权力机构整体上相信数字货币可以通过提供一份可以活动的记录而辅助执法机构，甚至解决一系列涉及金融服务和物联网的网络犯罪。《未来犯罪》（Future Crimes）的作者马克·古德曼最近称，“从未有一个计算机系统被证实为不可入侵的”。⁵⁹技术的发展也伴随着犯罪机会的增加。“一个人能够影响很多人的能力正在呈指数式增长趋势，而这其中有着良性和恶性的案例。”⁶⁰所以问题最终是关于人之间的互相伤害。犯罪分子会使用最新的技术去做这些事情。

不过，比特币和区块链可能会制约犯罪的用途。首先，犯罪分子也得将所有的比特币交易在区块链上公开，这样执法机构可以追踪比特币的付款，这比现金的追踪更简单。水门事件引出的“通过对钱的追踪找到坏人”的箴言实际上在区块链上更具备可行性（相比于其他的支付方式）。比特币的假名性质让监管者们有了可在将来用于起诉的信息，因为比特币比现金有更强的可追踪性。

在美国发生每一场大型的枪击事件后，美国国家步枪协会的持证会员代表很快就会说，“不要将美国的涉枪暴力怪罪到枪支头上！”如果是同样的一群人因其他人可能在区块链上实施的罪行而禁止区块链技术的话，那么确实会很有意思。技术并没有立场，它没有任何需求，也没有任何倾向。金钱也是某种形式的技术，当一个人抢劫了银行后，我们并不会怪罪“是金钱自己在保险箱里等着来抢”。罪犯对比特币的使用更多是与强力治理机制、监管、倡导及教育的缺失相关，而不是比特币的底层特性。

这是区块链将会失败的原因，还是实施过程的挑战？

这些障碍是令人畏惧的。眼前可以预见的障碍是量子计算机，它被认为是密码学家的“千年虫”问题。它将量子力学与理论计算结合用于解决问题，如用于密码学算法的破解上，可以比今天的计算机都快得多。史蒂夫·奥莫亨德罗称，“量子计算机理论上可以快速、高效地计算大型的数字，而大多数的公钥密码学系统都是建立在这样的任务基础上。因此，如果量子计算机真的有这样的能力，整个世界的密码学基础设施将会发生剧烈的转变。”⁶¹关于技术创新和进展的辩论由来已久：这个工具是善良的还是邪恶的？它对人类有益还是有害？就如讽刺作家詹姆斯·布兰奇·卡贝尔所观察到的那样，“乐观主义者认为我们生活在最好的世界中，而悲观主义者害怕这是真的”。⁶²

列弗·谢尔盖耶维奇·泰尔曼的故事表明，个人和机构可以使用创新成功去行善或作恶，从电力到互联网的范围很广的技术都说明了这一点。创意作品《网络的财富》的作者尤查·本科勒告诉我们，“技术在系统的层面上并没有偏向于不公平的因素，也没有对就业架构影响的偏向；那是属于社会、政治和文化的斗争。”技术可以剧烈地、快速地改变商业和社会，但尤查·本科勒相信这“并不是以一个已经确定的方式进行的”。⁶³

技术发展的历史总体上还是积极因素居多。考虑一下食物和药物产业（从研发、治疗和预防）里出现的进步：技术带来了更好的人类平等、生产力及社会进步。

不过，现在很难说区块链肯定不会重演互联网当初踏入的困局。它可能对中心化和控制是免疫的。但如果经济或政治上的回报足够多的话，强大的力量或许会尝试控制它。这个新型的分布式范式的领导者们需要证明他们的主张并开展经济及机构创新的步伐，以确保每一个人都

有机会参与在其中。这次，让我们履行其承诺。这就涉及了如何让这一切变为现实的问题了。

第十一章

下一代的领导者

21岁的维塔利克·布特因是一个出生于俄国的加拿大人，他是以太坊的创始人。之前有不少的人尝试用一些头衔去描述他，但“多产”这个形容词应该是最恰当的。（他是个多产的创始人）。如果你要问他的那群以太坊的追随者，他们会告诉你以太坊是一个“基于区块链的、任意状态的及图灵完备脚本平台。”¹它吸引了IBM、三星、UBS、微软、中国汽车巨头万向以及世界上最聪明的软件开发者的团队。它们都认为以太坊可能是能够改变一切事情的“星际计算机”。²

当维塔利克·布特因向我们解释“任意状态，图灵完备”时，我们了解到了他的一些想法。听音乐、读书或计算一天的收入和支出，这些事情的差异非常大，但你都可以在你的智能手机上去做这些事情，因为你的智能手机的操作系统是图灵完备的。这意味着它可以适应任何图灵完备的语言。因此，创新家们在以太坊上建造几乎是所有可以想象到的数字化应用程序，这些程序所执行的任务差异较大，范围包括了智能合约、计算资源市场、复杂金融基础设施以及分布式治理模型。

维塔利克·布特因是一个精通多种语言的人。举例来说，他能使用英语、俄语、法语、中文（他在假期里学了两个月）、古拉丁语、古希腊语、Basic、C++、Pascal、Java等。³“我的专长就是一般性”，他说道。他也是一个博学而谦虚的人。“我有这些不同的兴趣，而比特币像是一个完美的组合。它有数学、计算机科学、密码学、经济学、政治及社会哲学。我立刻被这个社区吸引了”，他说道。“我发现它真的能赋予人力量”。他在网络论坛上到处寻找，希望找到持有比特币的一些方法，最后发现了一个刚开始设立比特币相关博客的人。“那个博客叫

《比特币周报》，他当时正悬赏5个比特币让别人给他写文章。那时候大约是4美元的价值”，布特因说道。“我写了一些文章，赚了20个比特币。我将其中的一半花在一件T恤上了。走完了这整个流程，感觉差不多就像是在搭建构造社会基础的积木。”⁴

同样是这一个人曾经在大约5年前忽视过比特币。“大约在2011年2月，我爸爸跟我说，‘你听过比特币吗？它是一种只在互联网上存在的货币，而且没有任何政府背书。’我当时立刻想，‘是的，这个东西没有内生价值，它根本不可能成功。’”就跟很多青少年一样，维塔利克·布特因“在互联网上浪费了大量的时间”，阅读那些非正统的、非主流的理念。若你问他喜欢哪个经济学家，他很快地说泰勒·考恩、亚历克斯·斯塔巴洛克、罗宾·汉森以及布赖恩·卡普兰。他能说出博弈理论家托马斯·谢林及行为经济学家丹尼尔·卡尼曼和丹·艾瑞里的一些成果。“这是难以想象地有用，通过在论坛上与他人辩论政府等话题，你可以学习到很多。这就是一场很令人惊讶的学习历程”，他说道。比特币一直在发展。

在那年的年末，维塔利克·布特因每星期都花费10~12个小时为另一个出版物《比特币杂志》写稿。“当我还有8个月就进入大学的时候，我意识到它已经占据了我整个生活，那我还不如让它占据我整个生活吧。滑铁卢大学是一个非常好的大学，我也很喜欢那个课程。我退学的原因绝对不是因为大学不够好。而更多的是因为‘那个有趣，不过这个更有趣。’那是一个人生中只有一次的机会，我只是无法放弃这个机会。”他那时只有17岁。

在意识到区块链可以不仅有货币的用途，以及程序员需要一个与比特币区块链相比更灵活的平台后，维塔利克·布特因创建了开源的以太坊项目。以太坊允许在网络上同时实现高度开放和隐私的特性。他不认为这两者是矛盾的，不过“有点像黑格尔学说”，两者之间的辩证结果是“主动的透明性”。

就如历史上的很多技术一样，以太坊可能会取代一些就业职位。维塔利克·布特因相信这对很多技术来说都是正常的现象，并给出了一个新颖的解决方案：“在半个世纪内，我们将会放弃那种每天必需投入8小时劳动才能生存和享有体面生活的模式”。⁵不过，在区块链的问题上，他不认为大量工作职位的流失是不可避免的。以太坊可以为价值创造和企业家精神创建新的机会。“大多数技术都倾向于对一些外围的任务进行自动化运作，而区块链总是在中心进行自动化运作的”，他说道，“与其让出租车司机失业，倒不如说区块链让Uber失业并让司机可以与顾客直接交易”。⁶区块链并没有消灭工作机会，或许你可以认为它改变了工作的定义。谁会在这场重大的剧变中受伤？“与其他人相比，我估计（并希望）失业的是那些每年赚取50万美元的律师。”因此，维塔利克·布特因引用了莎士比亚的作品：“第一件事，让我们消灭所有的律师吧”。⁷

以太坊有另一个明显的矛盾。它是明显的利己主义并有着隐私的性质，但它依托于一个大型的、分布式的社区，这个社区以开放的方式为整体的个人利益的集合服务。确实，以太坊的设计精妙地捕捉了他对个体“会做正确的事情”这个恒久的信念，同时也配备了正确的工具以及他对社会中大型机构的动机的合理怀疑。虽然维塔利克·布特因对当代社会的问题所提出的批评非常深刻，但他表示仍存希望。“世界上有很多不公平的事情，但我逐渐地接受了世界的现状，并站在可能存在的机会的角度展开对未来的思考。”当他了解到3500美元可以让一个人在余生战胜疟疾，他并没有对来自个人、政府和公司的捐助的缺失感到惋惜。他想，“天啊，你只需要用3500美元就能拯救一条生命？这是一个非常好的投资回报率！我现在就应该捐助一些”。⁸以太坊是他将积极的改变作用于世界的工具。“我更多的将自己视为是改善技术为社会造福的整体趋势中的一员。”

维塔利克·布特因是一个天生的领袖，他用他的思想和愿景将人们

聚集起来。他是以太坊社区的主要的架构师及主要的共识达成者，也是一个由对任何与技术相关的事情都有着强烈看法的天才程序员所组成的更广泛社区的主要培育者。如果他成功了，将会对世界带来什么影响？

谁会领导一场变革？

在1992年，麻省理工学院计算机科学家戴维·克拉克说道，“我们拒绝国王、总统和投票。我们相信大致的共识和运行代码”。⁹这是第一代互联网的管理员的颂歌。这个声音是在当大多数人几乎无法想象互联网将会如何成为一种新型的人类沟通媒介，及超越在其之前出现的所有媒体对社会及日常生活所带来的影响时发出的。戴维·克拉的辞藻体现出了一一种与常规方式截然不同的，全球资源的领导与治理机制，并引出了一个非常有效的治理机制的生态系统。

从第二次世界大战结束后，国家本位的机构一直在管理全球重要的资源。其中两个最强大的机构，即国际货币基金组织和世界贸易组织是在1944年布雷顿森林会议上诞生的。联合国及世界卫生组织这样的联合国下属机构一直在全球问题的解决上有着垄断性的影响力。这些机构自身的设计就是层级化的，因为层级化是在那个饱受战争摧残的世纪的上半叶最具影响力的范式。不过这些产业规模的解决方案对数字时代面临的挑战来说是明显是不合适的。互联网的兴起是传统治理文化开始不再适应时代发展的一个重要标志。

在1992年，互联网上的大多数流量都是以电子邮件的形式发生的。让Tim Berners-Lee的得以实现其非凡的万维网的图形浏览器还差两年才能面世。大多数人并没有被连接起来，也不理解这些技术。很多原本可以逐渐掌管这项重要的全球资源的机构要么就处于萌芽阶段，要么就尚未出现。互联网工程任务组自成立起到那时候才经历了4年，这是一个掌管很多方面的互联网治理任务的国际社区。能够提供如域名管理这样

的关键服务的机构，即国际名称与数字地址分配机构(ICANN)，在那时候还差6年才成立。文特·瑟夫和鲍勃·卡恩那时候才刚开始招募人员来建立日后的互联网协会。

第二代的互联网的发展历程也体现出了开放性的热情及对层级体制的厌恶，这体现在中本聪、沃里斯、安德烈亚斯·安东诺普洛斯、绍博和罗杰·维尔等人的思想中。开源是一种重要的组织原则，但并不是一个带来进展的做法。虽然开源的方式已经在社会中让很多机构实现转型了，但我们依然需要协调、组织和领导能力。像Wikipedia和Linux这样的开源项目，虽然有着贤能统治的原则，但依然有吉米·威尔士和林纳斯·托瓦兹这样的“良性独裁者”这样的角色存在。

值得赞赏的是，中本聪将分布式权力、网络化的正直性、没有争议的价值、利益相关者的权利（包括隐私、安全性和所有权）以及包容性通过代码融入技术的设计当中。因此，这项技术在早期得以茁壮成长，逐渐绽放出我们今天所认识的生态系统。不过，这个无神论式的不干涉政策开始展现出其局限性。就如所有的颠覆性技术一样，在区块链生态系统里也有一些互相竞争的观点。即使是区块链的核心代表团也分裂成不同的加密技术阵营，每一个组织都在提倡各自的议程。

前白宫雇员及区块链倡导者、现在是MIT数字货币计划主管的布赖恩·福德说道，“如果你关注一下区块大小的辩论，那真是关于区块大小的吗？在媒体上确实是这样的，但我看到的也是一个治理机制上的辩论”。¹⁰这个生态系统需要什么样的模式或什么样的领导体制？迈克·赫恩是一个比特币核心的一个重要开发者，他在2015年1月发出的那篇预言了“比特币即将死亡”的告别信在产业内引起了一场轰动。在信中，他列出了产业所面临的紧迫挑战；这主要是指重要的技术标准问题仍然没有答案，而社区的队伍中也有不调和及迷惑的情况。迈克·赫恩的结论是这些挑战最终会导致比特币走向失败。我们对此表示不同意。迈克·赫恩将这些问题认为是比特币的致命缺点，但这篇文章在我们看来是一

一篇关于基于透明性、贡献和协作的多方利益相关者之间的治理机制的论文，其内涵意味深长。代码只是一个工具。若这项技术需要走向下一阶段并实现其长远的前景，人类必需进行领导。我们现在需要网络中的所有利益相关者聚集起来并关注一些关键的问题。

我们已经列出了一些摆在面前的障碍，它们是非常显著的。不过，这是这场变革要走向成功所面临的挑战，而不是反对这场变革的理由。直到今天，很多的问题依然没有得到解决，也缺乏一些集体行动去解决这些问题。这项技术应该如何继续进行扩展，而且是不对现实环境带来损害的前提下进行的？那些强大的力量会扼杀创新还是把它收入囊中？在不倒退到层级机制的情况下，我们将如何解决一些充满争议的标准相关的问题？

这就是我们在过去两年一直在研究的事情。我们发现，我们需要那些非国家控制的社会团体、私营企业、政府、个体的利益相关者的协作，而不能依赖国家本位的机构。我们将其称为“全球解决方案网络”（GSNs）。这些网络正在不断地成长，实现新式的公司、社会变革甚至是全球公共价值的生产。

其中重要的网络自然是互联网自己了。它的聚合、编排和治理是个人、社会团体组织及公司构成的协作关系所实现的，也会得到来自国家的隐性（有时是积极）的支持，而这样的协作曾经是不可想象的。不过，没有一个政府、国家、公司或国家本位的机构能够控制互联网。它是有效的。通过这样的做法，它证明了不同的利益相关者能够通过包容性、共识和透明性对一个全球资源进行管理。

这些经验和教训是很明显的。对这样复杂的全球创新成果进行良好的治理并不能只依靠政府去完成；我们也不能将这个任务交给私营部门，毕竟商业利益并不足以确保这项技术能够为社会服务。最终，我们需要全球的利益相关者一起协作并提供领导能力。

区块链生态系统：你无法在缺乏花名册的情况下分辨出参与者

虽然区块链技术最初是发端于开源社区，但它很快吸引了很多的利益相关者，每一类持有者都有不同的背景、兴趣和动机。开发者、产业参与者、风投家、企业家、政府和非政府机构有着各自的角度，也扮演着不同的角色。早期迹象表明，这些核心的利益相关者看到了对领导能力的需求并开始站出来了。我们重新看一些这些参与者是谁：

区块链产业先锋

从埃里克·沃里斯到罗杰·维尔这样的产业先锋都相信任何形式的治理、监管、管理或监督机制对比特币的原则来说不仅是愚蠢的，也是对立的。¹¹埃里克·沃里斯说道，“比特币早就被数学的原理监管得很好了，而数学原理是不会受到政府的干扰的。”¹²不过，随着产业开始扩张，很多企业家正在意识到与政府保持良好的对话及在更广范围内关注治理问题是一件好事。像Coinbase、Circle和Gemini这样的公司已经加入了交易组织；像MIT的数字货币计划这样的一些机构甚至保持着与新生的治理机构的密切关系。

风投家

这项技术刚开始是一群密码学专家的小圈子里的作品，很快获得了硅谷最大的、最耀眼的风投机构的关注，深受尊敬的Andreessen Horowitz亦是这些风投资本中的一员。现在，金融服务产业的巨人正在扮演着风投资本的角色：高盛、纽约证券交易所、维萨、巴克莱银行、瑞银和德勤已经直接投资到初创企业或那些培育新企业的孵化器里。养老基金也正在参与到这个领域中了。

加拿大安大略省雇员退休金计划是加拿大最大的公共机构养老基金

的投资部门，其规模达10亿美元，它在2015年做出了第一笔投资。主管该组织运营的吉姆·奥兰多正在寻找一种区块链的杀手级应用，它能够为区块链实带来“像网页浏览器作用于互联网”那样的意义。¹³从2012年的200万美元增长到2015年前半年的5亿美元。¹⁴这样的热情程度是非常明显的。蒂姆·德雷伯告诉我们，“金融家还在低估区块链的潜力。”¹⁵活跃的风投家们可以提倡这项技术，并支持一些新生的治理机构，如由Andreessen Horowitz提供资金的Coin Center.由巴里·西尔伯特创建的风投机构数字货币集团已经委任了一些学者和其他的一些非传统的顾问到其董事会，以通过投资和倡导这两个手段来加速一个更完善的金融系统的发展过程。

银行和金融服务业

在金融行业之外，我们还没看到过对一项技术的意见转变得如此快速的情况。长期以来，大多数金融机构将比特币视为赌徒和犯罪分子的投机工具并进行排斥，几乎没有将区块链放到眼中。今天它们都“全身投入”了。在2015年看着能够实时地看到这些事件的发生确实是令人难以置信。在2015年之前，只有很少的主流金融机构表示过参与了在该领域的投资。今天，澳洲联邦银行、蒙特利尔银行、法国兴业银行、道富银行、加拿大帝国商业银行、加拿大皇家银行、道明银行、三菱UFJ金融集团、纽约梅隆银行、富国银行、瑞穗银行、北欧银行、荷兰商业银行、意大利联合信贷银行、德国商业银行、麦格里银行以及其他数十家银行正在对该技术进行投资并参与到领导者的讨论当中。世界上最大的银行中的大部分已经参加了R3联盟，而更多的还参与到了Linux基金会以发起超级账本（Hyperledger）计划。银行应该被包含到领导者的讨论当中，不过其他的利益相关者必需警惕强大的现有机构寻求控制这项技术的可能性，就如他们在互联网发展的早期也对此进行谨慎处理一样。

开发者

社区中的开发者在基本上的技术问题上产生了分裂，而社区正在表达出一种对协调和领导者的需求。比特币核心开发者加文·安德烈森处于区块大小辩论的中心环节，他告诉我们，“我更倾向于待在引擎室里面，保持着比特币的引擎继续运行”¹⁶而不是花费大量的时间传播他的观点。不过，鉴于社区里缺乏明晰的领导者的现状，加文·安德烈森无心地走进了公众关注的焦点位置上。在2015年的夏天，他告诉我们，“我接下来6个月的工作是要专注于比特币的技术生命，确保比特币在未来的2~3年能够继续为下面这些业务服务：微支付、股票交易或产权转让以及所有的其他东西。”这涉及了很多的倡导和游说工作。对他而言，互联网的治理网络是一个很好的起点。“我总是在寻找榜样，而最典型的榜样莫过于互联网工程任务组。”¹⁷他认为互联网治理模式“有点无秩序和混乱”，不过它确实有效，而且也是可靠的。

学术界

学术机构正在资助实验室和各个中心以对这个项目展开研究并与它们机构外的其他同行进行合作。布赖恩·福德告诉我们，“我们发起了数字货币计划，以促使我们在MIT的一些优质的资源去关注这项技术，因为我们认为这在接下来的10年间是最重要的技术变革之一”。¹⁸MIT媒体实验室的主管伊藤穰一看到了这项技术对学术界的机遇并站出来了：“MIT和学术界可以作为一个评估、研究及讨论可扩展性这类问题的场所，而无须基于任何偏见或特殊的利益”。¹⁹这个领域中最重要的一位法律界知名人士杰里·布里托以前在乔治梅森大学工作过，现在是一个非营利性的倡议组织Coin Center的董事长，他说道，“治理模式会在需要就重要问题做出决定时发挥作用，而你需要有一个流程才能让实现这点”。²⁰他推荐从希波克拉底氏誓言（hippocratic oath）开始：首先，不能做出任何伤害。当前比特币核心开发者所采用的自下而上的方法“在区块大小的争议中展示出其不完善之处。这样将会很难获得任何共识”，杰里·布里托说道。“我们想帮助发展一个对话的场所，并在有

需要的时候培养一个自我监管的组织。”²¹一些知名的大学，如斯坦福、普林斯顿、纽约大可和杜克大学也开展了针对区块链、比特币和加密货币的课程。²²

政府、监管者和执法机构

全世界的政府在他们的行动上都是缺乏协调的，一些政府倾向于不干涉政策，另一些政府推行新的规则和监管规则，就像是纽约的BitLicense（数字货币牌照）。一些政府的态度显然是很敌意的，不过逐渐地这样的反应也是被边缘化了。同样地，根据对新规则的支持程度，产业也在分裂成各种派系。那些对来自政府的干预有所抵触的声音也承认政府参与到治理问题的辩论当中是有其积极意义的。产业内硕果丰富的风投家亚当·德雷珀不情愿地承认，“政府的支持带来了机构的支持，这是有价值的。”²³全球范围内的央行正采取不同的步骤试图了解这项技术。曾任纽约州金融服务局主任的本杰明·罗斯基称强而有力的监管是通往产业成长的第一步。²⁴

非政府组织

2015年被证明是对逐渐增加的、专注于这项技术的非政府组织和社会团体机构来说具有变革性意义的一年。虽然布赖恩·福德的数字货币计划是在MIT里面的，但我们也将它放这里了。其他类似的组织包括了杰里·布里托的Coin Center以及佩里安·博林的数字贸易商会。这些组织在社区中的影响力正不断壮大。

用户

用户是指你和我这类角色——那些关心身份、安全性、隐私及其他权利、长期可行性、公平裁决的人，还有关心纠正错误及与使用这项技术侵害我们利益的罪犯做斗争的人所组成的对话渠道。每个人似乎都

在基本的分类问题上有不同的意见：区块链是指比特币区块链还是指区块链这个普遍的技术？区块链的英文名称应该是Blockchain（大写字母开头的）还是blockchain（小写字母开头的）？它是一个货币、商品还是技术？它到底属于以上所有的类别中，还是根本不属于上述的范围？

区块链里的女性领导者

就如我们所观察到的那样，区块链运动中大部分人参与者都是男性。在技术和工程领域，男性参与者的数量还是显著地超出女性。不过，那些知名度高的女性开始在这个领域参与公司的创建与管理：数字资产控股的首席执行官布莱思·马斯特斯、Xapo主席辛迪·麦克亚当、Case Wallet的首席执行官梅拉妮·夏皮罗、恒星币发展基金会执行董事乔伊丝·金、BitPesa的首席执行官及创始人伊丽莎白·罗谢洛以及Third Key Solutions公司的首席执行官帕梅拉·摩根。她们中的很多人都表示这个产业对所有的参与者都非常欢迎，不管是男性还是女性。区块链领域的风投机构也开始以多样性的形式逐渐增加。前BitGo商业发展部门主管阿里安娜·辛普森现在是这个产业内的一个投资者。亚拉克·乔班普特拉是一个风投基金的投资者，它的基金现在专注于去中心化技术上。

在与这项全球资源的治理和管理有关的问题上，女性已经开始了主导作用。

普里马韦里·德菲利皮是哈佛大学Berkman中心的教职工及位于巴黎的国家科学研究中心的终生学者，她是一位孜孜不倦的区块链技术的倡导者，她的观点被认为是学术界在治理问题上最清晰、最有说服力的观点之一。她是一个在生态系统内相关对话的组织者、倡导者及推广者。康斯坦丝·蔡是产业内的另一位颇有名望的女性，她是从律师转型为企业家的，普里马韦里·德菲利皮与她一起在哈佛大学、MIT、斯坦福大学、伦敦、香港、悉尼等地引导出一批区块链工作坊。他们将产业内外不同的利益相关者集中起来以就重要的问题展开辩论。在这里，没有什

么事情是不能讨论的，而这些活动通常有很多具有不同背景、信念和信仰的人参与。

伊丽莎白·斯塔克是另一位在治理问题上的新星。这位耶鲁法学院的教授正扮演着产业内的最高召集人的角色。就如一位名望的女性——麦克阿瑟研究会会员、伯克利大学计算机科学教授以及网络安全专家唐·桑一样，伊丽莎白·斯塔克有着一个截然不同的学术背景，但她有其他的志向。她组织了比特币扩容（Scaling Bitcoin）活动，在蒙特利尔将开发者、产业参与者、意见领袖、政府官员和其他利益相关者集中起来。这就像是产业内的一个“立宪时刻”，人们认为这个活动打破了区块大小辩论的僵局。今天，她也以企业家的身份发挥着主导的角色，在比特币闪电网络（Bitcoin LightningNetwork）的开发中进行协调，以解决区块链可扩展性问题。

佩里安·博林之前是一位新闻工作者及电视台记者，现在是数字贸易商会的创始人，这是一个位于华盛顿特区的贸易协会。在一年时间内，这个组织吸引了一个知名度极高的委员会，如布莱思·马斯特斯、詹姆斯·纽瑟姆和乔治·吉尔德。她说，“这场运动需要有人在华盛顿与政府展开对话”。得益于她的新闻学方面的背景，佩里安·博林专注于传播、定位和优化相关的信息。她的组织“对每一个致力于社区成长的人都是开放的。”现在，她已经成了在迅速发展的区块链治理生态系统里的政策、主张和知识的领导者。²⁵

不断加入的领导者们纷纷就治理问题进行游说，是可以预见的，也是迫在眉睫的。当我们在讨论区块链技术的治理问题时，我们并不是单独地讨论监管的问题。其中一个原因是，使用监管的手段去管理这样的一项重要全球资源有着其严重的局限性。就如伊藤穰一所言，“你可以对网络进行监管，你可以对运作项目进行监管，但你不能监管一个软件”。²⁶因此，监管将会是几个重要的元素之一。区块链与互联网有着不同之处，因为金钱与信息差异很大。布莱思·马斯特斯演绎着华尔街玩

家到区块链先锋的极致历程，表达出其担忧：“新进来的参与者可以简单地做那些受监管的机构无法做的事情，不过在将顾客暴露到缺乏监管的金融活动并得出‘这是对顾客有利的’结论之前，人们必需仔细地思考一下，这些监管措施之所以存在的原因及其意义”。²⁷最终，这场辩论并不是关于我们需要一个什么样的社会的问题，而是关于领导者管理这个重要的全球资源的机会。

区块链监管的警世恒言

前任纽约州金融服务部主任本杰明·罗斯基曾经是美国权力最大的银行业监管者。华盛顿的内部人士都知道本杰明·罗斯基每天早上在市内短跑并拍摄自拍照的习惯。不过对华尔街的巨头来说，他是一个大胆的、野心勃勃的（还有过度热情的）打手，经常对任何他认为行为不检的银行展开斗争并让这些银行受到应有的惩罚。

本杰明·罗斯基是首个任职于对美国境内的特许银行实施监管的高级部门的人，当时是被他的朋友及长期政治同盟安德鲁·科莫委任的。英国渣打银行经手了来自伊朗的超过2.5亿美元交易，而这样的交易当时是属于美国及欧盟的所禁止的制裁范围内的。在2012年，他仅在这个职位上工作了一年，就因纽约州金融服务局与渣打银行所达成的价值3.4亿美元的和解协议而登上了新闻头条。在这个过程中，纽约州金融服务局的反应比寻求对该行为做出类似惩罚的司法部更快。²⁸对那些曾经认为银行监管相关事项非常松散的人来说，他就是新来的警官，也是在一个充满混乱状况的产业里的无畏的领导者及改革者。对银行来说，他迅速地成了头号公敌。那时候本杰明·罗斯基才刚开始而已。

在2013年中期，本杰明·罗斯基在办公室里可能还在准备另一件针对大型银行的轰动案件时，他属下的一名经济学家来到了他的办公室并讨论了一些不寻常的问题。根据外面一些律师所提供的情报，他们的一

些客户的公司正在交易一种奇怪的新型虚拟货币“比特币”。罗斯基的第一反应是“比特币是什么东西”？²⁹这个经济学家继续解释了那些公司有一些使用这种“数字美元”去购买、销售、交易和支付商品和服务的顾客，而那些保持谨慎的律师想知道这样的活动是否构成了金钱转账的定义，如果是的话应该怎么处理。在纽约，金钱转账通常是在州的级别进行监管的；这样，作为纽约州的监管者，纽约州金融服务局有责任监管任何进行金钱转账的实体。不过这该如何监管？本杰明·罗斯基都没有听说过这项技术，而他当时也产生了一丝疑虑，料想这是一种截然不同的挑战。

很快，本杰明·罗斯基面对着一个老生常谈的问题：颠覆性的技术并不能归纳到任何现存的监管框架里，而这是数字时代的一个特点。在他的观念中，比特币根本就无法归纳进来。比特币的影响范围是全球性的；而联邦和州政府部门只能在其范围能及的进行监管。还有，这项技术是点对点的及去中心化的。监管者的工作是实施对大型中介机构的监控。它们的中心化的账本存储了大量的数据，这对立案工作是很有用的。而在数字时代，政府官员很少能够得到与公众利益相关决定的决策所需的全部信息。在通常情况下，它们缺乏有效对新技术进行监管的资源，对创新也是孤陋寡闻。本杰明·罗斯基逐渐接受了数字化时代的政府及监管者们在过去20年间所面临的一些挑战。加密货币是数字化技术如何与包括政府在内的传统决策制定者争夺治理权的另一个例子。

不过，本杰明·罗斯基还是要履行职责的。在查阅了现有的法规后，他发现这些法律有着严重的不足。这个部门刚开始希望用美国内战时代写下的规则对这项技术进行监管。那些金钱转账相关的法律不可能考虑到任何形式的数字化技术（如互联网），更不用说加密货币或网络安全了。“随着我了解得越深入，我对这项技术的潜力产生了越来越强烈的兴趣，我也想象到了随着时间的推移，这项技术可以建造的各种应用程序和平台”，他说道。如果他“可以做好正确的监管，确保趋利避害并减少监管因素所带来的过多负担，我们就有机会帮助一个可能会给我

们的系统带来重大改进的技术成长”。³⁰本杰明·罗斯基总结道，“或许我们需要一种新型的监管框架以处理这种截然不同的事情的监管工作”？³¹他的提议BitLicense就是对产业进行监管的首个重要尝试。这是一个充满争议性的法规，它展示出了良好用意的监管可以带来不可预见的后果。当BitLicense生效后，大批的公司（如Bitfinex、GoCoin和Kraken）离开了纽约。它们认为这个许可证的高成本是它们离开的主要原因。那些还留下来的企业更多是那类资金雄厚的及更成熟的企业。

监管及顾客保护状况的改善有着显著的益处。像Gemini这样得到许可的交易所获得了更多的认可度，或许是因为它们的机构客户知道它现在已经像银行那样受到监管了。不过，随着竞争者数量的减少，BitLicense会否扼杀创新及抑制增长？杰里·布里托认为BitLicense将旧有的解决方案应用到新问题上的做法并不能达到目的。他引用了BitLicense的一条规则，内容是替客户托管资金的机构需要申请一个许可证。“像比特币和其他数字货币这样的东西，引入了多重签名的技术，由此也首先带来了分权控制的概念。这样，如果我们每一个人持有某个多重签名地址的‘2/3方案’的其中一个钥匙，谁是在托管客户的资金？”³²在这个案例中，在法律中曾经很明确的托管概念现在就变得模糊起来了。

“我认为接下来的5~10年将会是我们的金融系统最有动态、最有趣的时间段之一”，本杰明·罗斯基说道。³³他从纽约州金融服务局辞职，在这个动态的环境的中心地带继续研究各种复杂的问题。“如果我可以将时间花在我相信将会有着巨大变革、动态及有趣的时代，我将会很享受我的职业生涯.....你有一个由这个技术构成的世界，这通常是缺乏监管的，也与或许是最受监管的金融产业互相产生碰撞。没有人知道这场碰撞的后果是什么，”他说道。“接下来的5~10年应该就有结果了，而我希望在这场碰撞的中心点。”³⁴

那个可能会改变世界的参议员

这是加拿大参议院的一件惊人的举动——它的银行业、交易和商业委员会在2015年发布了一份题为《数字货币：你不能翻转这个币》³⁵的积极、深刻的报告。这份报告包含了来自区块链生态系统的多个参与者的反馈意见，并详细地指出了政府为什么应该拥抱区块链技术。³⁶

“这有可能成为下一个互联网”，来自亚伯达州的卡尔加里市的加拿大参议员道格·布莱克说道，“这可能会成为下一个电视机、电话机。我们想让加拿大内外都知道，我们支持创新和企业精神”。³⁷就如本杰明·罗斯基一样，道格·布莱克是一名资深的律师。他从该国的石油产业中塑造了其职业生涯，并作为加拿大最具盛名的律师事务所的合伙人之一为石油和燃气生产商服务。不过与本杰明·罗斯基不同的是，他不愿意过快推出监管政策。“政府应该不要拦路！”道格·布莱克告诉我们。³⁸作为加拿大参议院中的一员，他和他的同事并没有扮演正式的立法角色，不过可以通过向政府做出引导或建议的方式对重大的事项产生影响。加拿大参议院内的平均年龄是66岁，它不太可能倾向于拥抱这项前沿技术。但是，它们确实这么做了。

道格·布莱克回想了他在这个过程中的想法，“我们应该如何创建一个鼓励创新而不是扼杀创新的环境？.....对政府来说从一开始就考虑到这个角度并不是一件寻常的事情。”根据布莱克所说，政府“倾向于考虑保持控制及将风险最小化。”³⁹在意识到任何新技术对顾客和商业可能带来的风险时，道格·布莱克解释道，“做任何事情都是有风险的；法币系统中也有风险。我们可以在一定程度上管理风险，不过让我们也创建一个可以鼓励创新的环境吧。”⁴⁰道格·布莱克认为这份报告表示出他们已经命中了目标。

这份报告做出了一系列的建议，不过其中两条特别引人注目。首

先，是政府应该开始将区块链技术用于与加拿大人的互动中。道格·布莱克说道，“区块链是一个更具有机密性的数据保护载体”；因此，“政府应当开始寻求利用这项技术的方法，这会带来一个很有力的信息。”⁴¹这是一个很有利的声明：如果想成为某个领域的创新中心和先锋，你就应该将你的钱花在与你生计相关的问题上，并开始对自己进行创新。

第二条建议或许更令人惊讶：政府应当执行轻度监管的政策。一些关注区块链技术的人提出了这项论点，而他们在自己所在的法律专业中也是备受尊重的。美国叶史瓦大学卡多佐法学院的亚伦·赖特提倡一种“安全港”法律，以让创新家们在进行创新的同时减少政府的监管，直至该技术走向成熟为止。⁴²华盛顿和李大学法学院说道，“我们需要像技术那样的法律，有着谦逊、实验及迭代的特性。”⁴³

去中心化经济中的央行

金融或许是世界上第二个最古老的职业，不过央行是一个相对现代的概念。世界上最强大的央行——美国联邦储备委员会在2013年举行了成立100周年的庆祝活动。⁴⁴在相对较短的历史里，央行已经经历了多次的转型，最近的一次是从金本位到法定货币的浮动比率的体制。数字货币给央行在一个经济体中所扮演的角色带来了挑战，因此我们能够预料到央行的行长们会反对区块链技术。不过，在过去的一些年间，这些行长展示出了进行创新的意愿。在所有的支票都是以手工的形式进行结算和清算的时候，美国联邦储备委员会通过对自动清算所系统的支持成了资金清算电子化的先锋。就如任何其他地方的央行一样，美国联邦储备委员会也乐意进行实验。它拥抱了不合常规的及未经测试的政策，其中最毁誉参半的莫过于2008年金融危机时推出的量化宽松政策，那时候它使用了新铸造的货币去购买像政府债券这样的金融资产，其规模是史前未有的。

这并不奇怪，央行的行长们一直在超前思考区块链技术对它们各自的经济体的重要性。这是有两方面的原因的。首先，这项技术代表着一个能够改善金融服务产业的强大的新工具，很可能对大量的金融机构带来颠覆并增强央行在全球经济中的表现。

其次，另一个重要的原因，是区块链为央行带来了存在主义上的问题。它们应当如何在一个含有一种或多种它们无法控制的加密货币的全球市场中有效地行使其角色？毕竟，货币政策是央行的行长们管理经济的工具箱中的一个重要杠杆工具，特别是在发生危机的时候。如果货币不是由政府发行，而是作为一个分布式网络的一部分在全球范围内存在，那会发生什么事情？

世界各地的央行行长正在探索这些问题。加拿大央行副总裁、央行老兵卡罗琳·威尔金斯告诉我们，“我们对自己现在的范式非常有信心，但我们明白很多范式都有其适用期：它们将会以良好的状态运行很多年，然后就会开始出现问题了。你可以先在边缘修复这些问题，但最终还是需要切换到另一个范式中”。她相信区块链技术就是那“另一个”范式。“若要对这项具有如此变革意义的事物不产生着迷的感觉，那是非常困难的事情。这项技术可以用于某些方面的用途，对央行行业所有的职能都会产生影响。”她说道。⁴⁵

美国联邦储备委员会前任主席本·伯南克在2013年称区块链技术可以“带来一个更快、更安全及更高效的支付系统”。⁴⁶今天，美国联邦储备委员会和英格兰银行，还有一些可能尚未发出声音的其他央行行长，已经指派了团队专门负责对这项技术的研究。

若要理解央行行长本对此技术如此感兴趣的原因，让我们先理解下央行的职能。一般来说，这样的权威机构扮演着三种角色。首先，它们通过设定利率、控制货币供应量以及在特殊情况下将资本直接注入系统的做法进行货币政策的管理。其次，它们尝试维护金融稳定性。这意味

着它们扮演着为政府及金融系统中的各种银行提供服务的银行家角色；它们也是所谓的“最后贷款人”。最后，央行通常与其他政府实体分享监管及监督金融系统的责任，特别是那些与普通消费者打交道（涉及存款和贷款）的银行活动。⁴⁷这些角色总是相互缠绕、相互共存的。

我们先从金融稳定性进行分析。“作为一个央行，我们的角色是最终的流动性提供者。我们对加拿大元是这样做的。因此，加拿大元对加拿大金融系统来说是一个重要的流动性来源”，卡罗琳·威尔金斯说道。如果交易是以另一种货币（如比特币）的形式发生，那会是怎样？“我们作为最终贷款人的能力将会受到限制”。⁴⁸这会有哪方面的解决方案？央行可以简单地开始将比特币作为它们的储备，就如它们对待其他的货币和资产（如黄金）一样。它们也可以要求金融机构将这些非国家发行的货币托管到央行中作为储备。这些储备将会让央行可以同时的法币和加密货币体系中执行其货币政策。这听上去很谨慎，对么？

当考虑到与货币政策有关的稳定性时，卡罗琳·威尔金斯声称“电子货币的货币政策的影响取决于它是如何计价”。她在最近的一场演说中建议了“电子货币可以由政府以国家货币或加密货币的形式计价”。⁴⁹她说，一种以加拿大元计价的数字货币将很容易管理。它甚至可能帮助一个央行实现更快的反应速度。最有可能的情况是，我们将会看到两者的结合：央行将会持有及管理另类的基于区块链的货币，就如它们处理外汇储备一样，而且将会通过探索通过基于区块链的账本去将法币转换成所谓的电子货币的做法。这个新世界看起来将会是截然不同的。

还有，央行作为监管者和监督者的角色将如何处理？它们在各自的国家中有着相当的监管权力，但它们并不是独立行动的。它们与其他的央行、金融稳定委员会、国际结算银行、国际货币基金组织和世界银行等其他全球机构进行协调和协作。我们需要更强大的协作行动以处理区块链技术的相关问题。今天，央行行长们在提出重要的问题。卡罗琳·威尔金斯说道，“人们可以轻松说监管应当与问题相适应，但这个问题

是什么？还有，我们想要哪方面的创新”？⁵⁰这些是我们能够在包容的环境中进行高效地处理得好问题。

布雷顿森林会议是一个很好的模式。能不能设立一个类似的会议，将思考者们都召集起来，提供一个包括私营部门、技术社区、治理机构在内的不同利益相关者都可以参与的公开论坛，而非是在充满烟雾的密闭房间进行沟通？卡罗琳·威尔金斯说道，“加拿大央行在理解这项技术及其意义的问题上有与其他的央行合作。我们举行了一些会议，邀请了各国央行、学者及私营部门的人来参加”。⁵¹

确实，央行的故事展示出一个更大的问题：政府通常缺乏应对一个快速改变的世界所需的知识。央行行长们确实有着对这场讨论来说非常重要的观点，不过他们应当将目光投到网络中的其他利益相关者及全球的其他央行以分享想法、在实质性的领导机制问题上进行协作并推动议题的前进。

监管与治理的对比

价值和金钱与传统的信息并非一回事。我们讨论的是储蓄、养老金、一个人的生计、她的公司、她的股票投资组合以及她的经济，而这些对每个人都有影响。难道我们不需要尽快有监管方案吗？政府能够（应该）在这场即将来临的重大变革前表现出克制吗？

重要的变革正揭示出政府在一个创新加速的时代的局限性。例如，200年的金融危机展示出全球经济系统的速度和复杂性让传统的中心化决策制定和执行变得越来越没有效果了。不过更强的监管体制并不是解药。政府不能指望监察和监管金融市场、技术或经济的每一个角落，因为里面的参与者、创新成果和产品实在是太多了。这场经验倒是说明了政府至少可以推动透明性以关注市场行为及带来改变。政府可以要求银

行的运作在网络上更透明，并让公民及其他参与方可以贡献各自的数据和观察结果。公民也可以帮助监管的执行，或许是通过改变他们的采购习惯，或通过以信息武装自己及组织公共活动来揭露出违规的行径。

当然了，政府必需是治理领域的重要利益相关者和领导者。它们必需意识到它们在区块链的治理中所扮演的角色与其传统的货币政策及金融监管中所扮演的角色是截然不同的。在千禧年，国家有着对货币的垄断力量。如果货币不再是单独有一个中心化的权力机构发行，而是由一个分布式的全球点对点网络创建的（至少一部分是），那情况会是什么样？

在保持总体的积极态度的同时，美国的回应有时是很矛盾的。“在美国，从国会到行政分支再到包含执法机构在内的不同机构都意识到这项技术有着重大的、正当的用途”，杰里·布里托说道。⁵²确实，互联网已经给我们说明了，美国政府的性情及机构设置使得它不仅能够容忍甚至欢迎触及其边界的创新成果。它也会通过监管制度妨碍创新——有些是被误导的，有些几乎肯定是过早的。

在确定掌握其意义之前过早地进行监管会产生深远的影响。在维多利亚女王时代的英国，所谓的自动驾驶机车（如汽车）必需根据法律的规定由一个站在它前面并挥舞着一面红色旗子的人陪伴着，以让旁人及马匹注意到这个即将来临的奇怪机器。产业中的领先企业GoCoin的首席执行官史蒂夫·博勒加德描述了过早监管的误区：“当网页刚开始出现的时候，监管者们那时候在尝试决定网页应该归属哪个部门来监管。其中一个想法是让那些搭建和维护网站的人去申请一个无线电带宽许可证，因为你们是在进行广播。你能想象到申请一个无线电带宽许可证才能建设一个网站吗？”⁵³幸好，这件事从来没有实现过。

我们要明确一点：监管与治理是不同的。监管是关于将法律设计用于行为的控制。治理是关于管理、协作及以共同利益的出发点行事的动

机。不过经验告诉我们应该谨慎地进行技术的监管，应该作为与其他社会部门的平等协作对象，而不是作为强势的法律执行者。它们可以作为一个自下而上的治理生态系统的参与者，而不是作为一个自上而下的控制体系的执行者。

Coin Center的杰里·布里托认为政府应该会有一些角色，但它们应该保持警惕。它提倡多个利益相关方的解决方案，这是从教育开始的：“在国会、机构、媒体进行讲解，回答它们的受众所提出的任何问题，或让那些能够聪明地回答这些问题的人与他们进行沟通。”⁵⁴

区块链治理的新框架

政府可以通过提高透明性和促成公民参与的方式改善产业的行为，而不是简单地进行监管。这并非一个更好的监管方案的取代措施，而是作为现有系统的一种补充。我们相信来自一种多个利益相关方的有效监管及治理，会更重视透明性和公众的参与度，并将这些因素考虑到决策制定当中。在这是人类历史上，这是由多个（非国家性质的）利益相关方的网络去共同解决全球问题的首次尝试。

在最近几十年，来自两方面的重要进展为一种新模式提供了基础。首先，互联网的出现为所有大小的利益相关方（可以细化到个人）创造了互相沟通、贡献资源及协调行动的方法。我们不再需要政府官员将我们召集起来以让我们的目标和努力一致。其次，商界、学术机构、非政府机构以及其他的一些非国家的利益相关者已经得到了在全球协作行动中扮演重要角色的能力，而在当年的布雷顿森林体系中并没有商界、非政府机构或非国家的利益相关者的参与。今天，这些利益相关者定期与政府进行交流以解决社会各方面存在的问题——从互联网这样的全球资源的治理到像气候变化和人口贩卖这样的全球问题的解决。

这些发展成果的结合让新的模式成为可能。针对那些日益增长的全球性挑战，自我管理的协作组织可以实现全球的协作、治理和问题解决，以及获得比传统的国家主导的机构更快、更强大的进展。

在考虑区块链治理网络的基础时，我们指出了一系列的关键问题，并设计了一个解决这些问题的框架：

- 我们应该如何设计这样的治理网络？
- 我们应该从头开始建设一个新的网络，还是围绕着一个现有的机构（已经有处理国际金融问题的支持者）搭建网络？
- 这个网络的会是谁来授权的，它有能力实施和执行政策吗？
- 区块链治理网络会为谁的利益服务，以及对谁负责？
- 关键的问题是，国家会真的放弃一个全球网络里的任何权力吗？

总体上说，互联网的治理生态系统充满了丰富的经验。它在短短的时间内成为一个全球资源的表现是令人震惊的，这得益于强大的领导能力和治理机制——虽然一些强大的力量对此表示反对。

那么，谁在治理着第一代的互联网，还有如何治理？这是一个由公司、社会团体机构、软件开发者、学者和政府（主要是美国政府）以一个开放的、分布式的及协作的方式所构成的广阔生态系统，这是传统的命令与控制式的层级体制及框架无法对比的。没有政府或政府组织可以控制互联网或其标准，不过一些美国政府部门曾经提供过资助。[55](#)

在互联网的早期，政府展示出了克制和预见性。通过在互联网革命中限制监管的程度，它们表现出克制；通过在引入新的规则和监管措施之前让生态系统茁壮成长，它们表现出预见性。这个多个利益相关方的网络对互联网是有效的，不过我们需要意识到区块链将会有有一个更强大

的监管角色。互联网带来了信息的民主化，区块链技术带来了价值的民主化并对传统产业（如银行业）的核心带来了冲击。很明显，将会有一些监管角色去确保顾客和公民是受到保护的。不过，我们的研究表明互联网治理模式是一个很好的模板。

到底有多少的领导者是来自过去的互联网治理社区？文特·瑟夫与其他人共同发明了互联网，并引导了互联网协会及互联网工程任务组的创建过程，而这个任务组几乎创建了所有重要的互联网标准。⁵⁶文特·瑟夫称区块链技术的一个很好的起点是在互联网工程任务组里创建一个同好交流会兴趣小组。在刚开始的时候，很多参与到互联网治理的组织将数字货币和区块链技术看成是在他们的权责范围外，不过这已经开始发生改变。万维网联盟已经将网页支付安排为优先项目，而区块链在该项目的讨论是处于中心的位置。⁵⁷还有，互联网治理论坛（IGF）已经主持了一些关于区块链和比特币的讨论，参与者探索了一些可以由此项技术实现的新型去中心化治理框架。⁵⁸新旧事物之间的边界是不断变化的，而互联网治理网络里的很多领导者，如互联网的先锋、前任ICANN副主席、互联网协会受托人黄平达已经成了区块链治理领域最高效的领导者之一。⁵⁹

这个新的治理网络将会是什么样子的？这里面有10个类型的全球解决方案网络。每一种都涉及公司、政府、非政府组织、学者、开发者和个人的组合。它们并不是由国家或国家本位的机构（如联合国、国际货币基金组织、世界银行或G8）所控制的。它们都将会在区块链技术的领导及治理中扮演一个重要的角色。



图3 全球解决方案网络

1.知识网络

知识网络的主要功能是开发可以帮助解决全球问题的新的思考、研究、想法及政策。那些见多识广及精通技术的用户可以更好地保护自己免受欺诈和盗窃的伤害，并保护自己的隐私。他们也可以实现这项颠覆性技术的完整价值，创造在全球繁荣及全球金融连通性中分享更多成果的机会。⁶⁰知识网络必需培育一个开放及包容的文化，增加透明度，并让多个利益参与方加入到其中。

对区块链的意义：知识网络是将新的理念扩散到其他全球解决方案网络及更广阔世界的起点。它们是避免陷阱和障碍的关键。知识将会让利益参与方准备好，以更高效地进行倡导、创造或共同创造政策以及向用户传播关键的信息。知识分享也能带来与政府之间的富有成果的对话。根据Coin Center的杰里·布里托所说，不管特定的政策问题是什么，如果政府“不理解这项技术及其影响，它们就注定走向失败”。⁶¹很多人提出了为各种理念和信息的分享创建更多空间的想法。“应该有一个论坛可以用于展示提议或理念”，泰勒·文克莱沃斯说道。⁶²MIT的数字货

币计划是一个领先的知识网络，试图团结及激发世界范围内的学者及高校参与到这个技术中。此外，还有一些不太引人注目的非正式聚会也在发生，如旧金山及纽约的开发者聚会，也让知识的优先级提高了。

Blockchainworkshops.org是另一个将利益相关者召集起来以传播知识和关键课程的组织。在线论坛及社区Reddit也是一个在领域内传播新知识的起点。

2. 投递网络

这类的网络实际上会投递它寻求的改变，能够补充甚至绕过传统机构的功能。例如，ICANN在互联网治理网络中扮演中重要的角色，以域名的方式投递解决方案。

对区块链的意义：我们如何确保有着足够的激励机制推动分布式大规模协作并确保该项技术做好被大规模使用的准备？我们可能会有区块链的“ICANN时刻”，即一些机构将会被设立以提供关键的功能。不过，鉴于ICANN和互联网治理网络中的很多全球解决方案网络组织都是美国的，领导者需要推动这些组织的国际化。伊藤穰一说道，“我认为现在已经存在将治理模式‘去美国化’和国际化的努力，这是在一开始就进行的，因为我们从ICANN的历史中学到了，如果你刚开始的时候你有一些美国的成分，你就很难脱离美国了。”⁶³

法律应用自动化联盟是一个扮演着几个关键角色的全球组织：它负责传播知识、影响政策、为区块链发出倡导及支持基于区块链应用程序的开发和部署，这些对主要潜在障碍的解决都是非常关键的。⁶⁴

3. 政策网络

有时候网络能够创造政府政策，即使这个网络中的一些成员可能是由非政府的参与者构成的。政策网络可以支持政策的发展或为政策创建代替方案（不管政府是否支持）。政策网络的目标并非从政府手上夺取

政策制定过程的控制权。相反，它们的目标是将决策制定从传统的层级化传播模式变成咨询和协作的模式。

对区块链的意义：今天，一个新生的政策网络正在呈现。Coin Center是华盛顿的一个非营利性政策组织，专注于五个方面：创新、消费者保护、隐私、许可证及反洗钱/了解你的客户。数字货币商会是一个贸易组织，它专注于倡导数字货币的接受及使用。⁶⁵英国有属于自己的数字货币协会，澳大利亚及加拿大也有，它们会为该产业发言。在聘用了前美国政府高级顾问John Collins后，Coinbase成为首个引入固定的政策主张角色的公司。⁶⁶在政策领域实施相应的推动将会确保区块链更有可能实现其潜力。例如，我们知道挖矿会消耗很多的能源，而气候变化是一个很大的问题。负责任的政策对建造一个可持续发展的未来是很有价值的，而政府并不能在这个事情上单打独斗。

4. 倡导网络

倡导网络寻求改变政府、公司或其他机构的议程或政策。互联网降低了协作的成本，而今天世界正见证着日渐强大的倡导网络的急剧兴起，这些网络是全球性的、大范围分布性的及具有非常复杂的技术。

对区块链的影响：倡导网络是随着人们对传统政治及社会机构的失望而兴起的，这使它们对区块链社区十分合适，同样是尝试颠覆传统机构解决问题的方法。不过，在这些早期的日子中，倡导网络必需作为政府的合作伙伴。倡导网络与政策网络有着紧密的联系，因此Coin Center和数字货币商会在这个领域冲在最前面就是意料之中的事情了，还有COALA、MIT的数字货币计划以及其他的一些组织。倡导对区块链技术的扩展是很重要的。如果没有强而有力的倡导行动去支持利益相关者及其权利，政府及其他强大的机构可能会尝试扼杀、扭曲或夺取这个强大的开放网络为自己的利益服务，这也是其中一个潜在的障碍。

5. 监察网络

这些网络会对机构实施细致的监察，以确保它们的表现良好，其主题包括人权、腐败、环境及金融服务相关的事项。在这个过程中，它们推动公共辩论，提高透明度并促进带来改变的运动。监察网络的角色自然是与倡导网络及政策网络互相缠绕在一起的。政策网络与政府进行协作以带来合适的政策。监察网络确保产业与政策相符合并实际上监督及执行合规工作。那些滥用公众信任的政府也可以被仔细监察并承担责任。

对区块链的意义：区块链联盟（Blockchain Alliance）是执法机构、非政府组织、贸易组织、私营部门等团队的合作伙伴关系，它是产业中第一个真正的倡导网络。Coin Center及数字贸易商会在Bit-Fury、Bitfinex、BitGo、Bitnet、Bitstamp、Blockchain、Circle和Coinbase等机构的支持下，与美国司法部、美国联邦调查局、美国特勤局、美国国土安全局等执法部门建立了合作关系。就如我们在前面的章节指出的那样，区块链在大范围内被罪犯利用将会是一个前进的障碍。这些监察网络也扮演着重要的倡导角色。在巴黎恐怖袭击发生后，欧洲的一些立法者、监管者和执法机构将比特币当成是恐怖主义融资的源头。区块链联盟让大家保持耐心：“不要因为恐惧而进行监管⁶⁷。”就在本书行文之际，我们不知道区块链联盟的倡导发挥了多少作用，不过可以肯定的是如果没有它们的参与状况可能会更糟糕，因为那样就只有政府在单方面处理了。除了有一些社区成员扮演着自我管理角色并在论坛及Reddit上召集讨论、进行协作和参与辩论，很少有其他监察网络参与进来。在刚开始，与执法部门建立合作关系是很有用的，不过区块链生态系统需要完全独立的机构，像一些传统的监察机构。否则，我们可能会成为另一个障碍的受害者：区块链可能会成为一个新型和强大的监视工具。

6.平台

数字化时代让机构可以比封闭、孤立的模式做得更好：它们也可以成为价值创造、创新及全球问题解决的平台。像change.org这样的机构

让个人可以发起从人权到气候变化等一系列议题的支持活动。“请愿平台”可以利用数百万人的协作力量并让他们的激情带来持久的冲击力。开放平台可以应用在很多问题上——从气候变化到区块链。⁶⁸

对区块链的影响：随着区块链技术的系统重要性增加，利益相关者必需收集和监察数据。比特币区块链或许是极度开放、透明及可调和的，但在从金融服务到物联网这些领域使用的封闭式区块链就未必是了。想象一个能让普通的公民收集和监察数据的平台，它是一个解决可扩展性的障碍、政府侵犯或不可持续的能源使用等方面问题的有力解决方案。它将能让监察网络和倡导网络促使机构和公司更负责任并推动有建设性的讨论。

7.标准网络

标准网络是非国家本位的组织，它的任务是为几乎所有的事物开发技术规格和标准，这包括互联网所用的标准。他们决定产品底层开发的标准，并允许有潜力的创新成果发扬光大。若全球标准网络需要实现其目标，它们必需利用个人、机构、民间团体组织及私营部门企业（这个是最重要的）的专长。互联网工程任务组是互联网治理网络的最主要的标准机构，它在整合来自不同利益相关者观点的工作上做得比较出色。

对区块链的意义：最初，比特币基金会资助了比特币核心协议（由社区使用的共同标准）的开发。不过，这个基金会将近解体的状态（由管理不善及浪费导致）证明了网络化治理解决方案的必要性。在意识到这项技术的深远的重要性及其对细致管理和培育的需求后，MIT创造了数字货币计划，它为比特币核心开发者提供了资助使得他们可以继续其工作。“我们立刻介入并在MIT媒体实验室为他们提供了职位，这样他们可以继续独自地继续支持比特币的核心开发。”布赖恩·福德说道。⁶⁹对核心开发者而言，能够自主地工作对核心协议的设计是非常重要的。

加文·安德烈森是在MIT工作的核心开发者中的一员。他相信若要在共同标准（如饱受争议的区块大小问题）上推动议题前进，是需要有领导者的。“或许你能让一个委员会设计某种五金工具的标准，但你不能用这样的方法设计软件标准，”他说道。当谈及网络发展的早期时，安德烈森说道，“互联网模式展示出在共识达成的场合可以有技术的出现，即使那时候缺乏明确的领导者，但你最终还是需要有一个个人或流程（最终还是由人结束）。你始终需要其中之一。”⁷⁰共识机制自身并不足以支持标准的开发。

Scalingbitcoin.org是一个将工程师及学者召集起来以解决主要技术问题的组织，其中包含了标准的问题。黄平达是Scalingbitcoin.org计划委员会的主席（这只是他其他的重要的领导角色之一）一直是产业里的关键领导者，他持续地将关键的利益相关者召集起来并清除产业中的重要障碍。在金融服务业，R3和超级账本项目都在致力解决重要的标准问题。最终，将会有不同事情上的标准网络，涵盖构建未来金融服务产业基础的区块链协议到物联网里的构造隐私和支付技术的共同标准。

这些组织从不同的角度、不同的立场试图解决问题，每一个组织都分享着让这项技术走向大规模使用的共同目标——构建基础设施、开发标准及使其可扩展。

8.网络化的机构

一些网络提供了广泛的职能，我们将其描述为“网络化的机构”。它们并不是国家本位的，但确实是真正的多个利益参与方的网络。它们创建的价值包括知识、倡导和政策，还有提供实际的解决方案。

对区块链的意义：世界经济论坛是一个领先的网络化机构，它一直是区块链技术的公开支持者。区块链技术是2016年1月达沃斯（世界经济论坛）的重头戏。世界经济论坛的金融创新领导人杰西·麦克沃特斯相信区块链技术是一项通用的技术，就如互联网一样，我们可以创建更

高效的市場及改善對金融服務的獲取。該組織預計在10年內我們將可以在區塊鏈上存儲10%的全球GDP（國內生產總值）。⁷¹作為一個組織，世界經濟論壇帶領了重大事項的改善和解決，如收入不公平、氣候變化甚至是匯款等問題。其他網絡化的機構，從最小的小組到世界上最大的基金會，如克林頓基金會及比爾蓋茨與梅琳達基金會，若它們使用這項技術去改善金融包容性及醫療保健服務等方面的重大議題，那將會是很明智的。網絡化的機構通常在影響政府政策制定的過程中扮演著一定的角色，讓其成為在一系列主要障礙的解決過程中成為關鍵的環節及戰略伙伴。

9. 僑民

僑民組織是由離開祖國及被文化和對祖國認知所團結起來的人們所組成的全球社區。得益於互聯網所提供的幫助，這些人及相關機構可以在多個利益相關方的網絡中進行協作。今天很多的僑民組織的功能之一是關注及幫助普遍的全球性問題的解決。

對區塊鏈的意義：僑民組織對區塊鏈的未來是很關鍵的。第一，區塊鏈使得發送匯款的过程变得更簡單及更可負擔。區塊鏈離所謂的“就業職位殺手”還差很遠，區塊鏈實際上為這些人創造了更多的時間和資源去追求其他賺取薪資的機會或創業機會。雖然在菲律賓和肯尼亞已經有一些公司在做這些事情了，但僑民組織必需做出更多的事以加速區塊鏈支付方法的認知、採用及接受程度。今天，在針對這個機會的公司（如Abra及支付機構Paycase）中，大部分是以美國、英國、加拿大或中國為基地的。

10. 治理網絡

區塊鏈治理網絡應該包含其他9個全球解決方案網絡類型的所有特性及屬性。最終，一個區塊鏈治理網絡應該力求具備包容性，並歡迎來自所有的利益相關方組織的參與。這個網絡應該是一個賢能治理的網

络，即社区会在可行的提议中进行遴选，而不考虑提议者的职衔或身份。网络应该是透明的，将其所有数据、文档及会议记录公开并接受公众的监察。最后，决策尽量要根据共识达成，以为其结果增加更多的合法性。

下一个数字时代的新议程

区块链治理网络对这项全球资源的管理至关重要。不过我们如何能确保这个下一代的互联网实现其潜力？数字时代的下一个纪元将会带来无限的可能性、显著的危险性、未知的障碍、艰难的挑战及不确定的未来。技术（特别是分布式的）为每一个人创造了机会，不过其结果最终是由人类决定的。

咨询机构负责人康斯坦丝·蔡认为，“这项技术有着其前景及危险性。主要是我们如何利用它”。⁷²就如这一章所讨论过的那样，每一个人都可以参与进来，实现数字时代的新愿景。在之前的划时代转变中，社会采取措施引入新的理解、法律及机构。这些文明的转型是需要时间的，通常是上百年，通常还会被冲突甚至是革命所中断。

今天的情况有所不同，因为改变发生得更快。更重要的是，摩尔定律表明改变的速率正在以指数级增长。我们正面对一个谚语中的“国际象棋棋盘上放谷子”的问题，即不断叠加的指数级增长有着不可思议的效应。⁷³结果是，我们的监管及政策基础设施是有着严重不足的，对数字时代的要求适应得太慢或根本没有适应。今天的颠覆影响变得越来越快，正超出了个人和机构的理解能力，更不用说管理它们所带来的冲击了。我们的民主机构和工具是为工业时代而设的——实际上它们是起源于农业化封建社会到工业化资本主义国家的转变过程中。

我们如何让人类转型的节奏更快，以适应加速中的技术创新和颠覆

性成果的步伐？为了不让别人将我们称为技术绝对论者或乌托邦空想者，我们是否可以指出现在已经是为数字时代设立新的社会契约的时候了。政府、私营部门、社会团体和个人需要一切协作以打造这个新的共同认知。

随着我们步入这个第二代的互联网，需要有一个为数字时代而设的宣言。可以将其取名为《互相依赖宣言》。数字时代的公民有访问数字化基础设施、文化、媒体识读、终生学习的权利，以及在网络上进行沟通而无须担心被监视的权利。

数字经济和社会应该根据原则来治理。确实，那些付出劳动的人应该分享到它们所创造的财富。如果计算机可以承担工作量，那么每周的工作就不再是生活的标准了，人类的工作时间应该减少了。实际上，中本聪为比特币提供的隐含设计原则也可以为我们很好地服务，我们需要能够根据正直性、安全性、隐私、包容、权利保护及权力分散等原则行事的机构。让我们一起将机会传播和繁荣从源头传播出去，而不是在财富被创造后根据传统的阶级架构简单地重新分配出去。

区块链技术或许能降低政府的耗费和规模，不过我们在很多领域依然需要新的法律。知识产权和权利所有权面临的挑战应该有技术和商业模式上的解决方案。因此，我们应该重写或废弃那些因对专利过度保护从而扼杀创新的旧法律。更完善的反垄断行动或许会阻止垄断化的趋势，这样没有人需要在如互联网或金融服务上付出过多的代价。80%的美国人对于互联网服务提供商并没有选择权，这或许可以解释美国的宽带条件是发达国家中最慢的、最昂贵的。那些操纵从外汇到柴油排放量等事项的犯罪操作分子应该被起诉和得到相应的惩罚。

我们将需要横跨不同领域的机构性转型。央行需要改变它们在货币管理和货币政策中的角色，并与经济和社会中更多的利益相关者进行多边协作。我们需要学校和大学为学生提供定制及协同制作的区块链相关课程，让学生和教师可以参与到小组讨论和项目当中。我们需要一个区

区块链上的统一医疗记录，以确保我们可以在系统外管理自身身体状况时实现医疗保健的协作。当我们进入医疗保健系统时，我们不应该因为对药物反应的无知或不对症的药物而受到伤害。政治家们需要适应一个透明的世界，这里面智能合约会确保他们对选区负责。在数字货币为5000亿美元的汇款市场带来冲击后，我们应该如何应对？

区块链技术可以实现新型的实体基础设施，这需要新的合作伙伴关系及利益相关方之间的理解。当Suber夺走了几百万Uber司机的职位后，会发生什么？城市如何确保在2025年市民会对其智能交通系统有着积极的态度？我们如何实现一个分布式的区块链电力网络，房产持有者不再仅仅是电力的消费者，还是电力的贡献者？我们将如何寻找实施区块链个人碳排放交易系统所需的领导力量？

可信的协议和你

范式转型的规律——旧范式的领导者是最难拥抱新范式的人群，在这次的转型中还会是这样吗？考虑一下那些曾经推崇过唐塔普斯科特在1994年写的《数字经济》一书的领导者：Nortel Networks、MCI、Nynex、Ameritech及GE Information Services（GE信息服务）公司的CEO们，这些人都已经销声匿迹了。起码他没有将Kodak（柯达）、Borders、Blockbuster或Circuit City的CEO包含在其中。（这对《区块链革命》的善意支持者来说是一种警惕）。

为什么鲁伯特·默多克没有创建《赫芬顿邮报》？为什么AT&T没有创造Skype？为什么Visa没有创造Paypal？CNN其实是有可能创建Twitter（推特）的，因为对它来说其实就是新闻摘要，不是吗？GM或Hertz也可能发起Uber、Marriott和Airbnb；Gannett也可能创造出Craigslist或Kijiji；eBay也可能发起Yellow Pages（黄页）；微软也拥有创造Google等其他的一些基于互联网（而非个人电脑）的商业模式的可

能性；NBC（美国国家广播公司）也可能发明YouTube；Instagram和Pinterest发明的时候Kodak在哪里呢？如果《人物周刊》或《新闻周刊》发明了BuzzFeed和Mashable，该会是什么样子？

就如我们在本书开头的时候所写的那样，“就如历史上反复出现过的场景那样，技术的小精灵似乎又一次从瓶子中被释放出来了……现在，这个小精灵或许能为我们所用，带来另一场变革，这将可能革新经济格局和人类社会各种事务的旧秩序。前提是如果我们能很好地利用它”。就如第一代的互联网，区块链革命有着颠覆商业模式及为产业带来转型的潜力。不过这仅仅是一个开始。区块链技术正无可避免地将我们带到一个新的时代，这个时代是以开放性、价值、去中心化和全球参与为基础的。

我们预计会有一段时间的不稳定性、投机性和滥用。我们也预期未来有着一个稳定的发展前景。现在还没有人意识到这个技术在金融服务产业会带来什么样的影响。本·罗斯基所说的“这个产业在未来的5~10年将会有翻天覆地的变化”是对的吗？蒂姆·德雷珀说道，“比特币与美元的对比就像是互联网跟纸张的对比”。⁷⁴那些最热心的区块链技术支持者会不会低估了它的长远潜力？区块链技术会不会是自复式记账法或股份制公司诞生以来对产业效率和价值的提升作用最大的技术？赫尔南多·德·索托称区块链有望将50亿的人口带到全球经济当中，让国家和公民之间的关系变得更好，及成为一个为全球繁荣而设的新平台及个体权利的保护者。对他而言，“通过法律实现和平、全球人类同属一个家庭的理念，有赖于我们在共同的标准上达成协议。我们应该思考区块链能否为《世界人权宣言》的实施提供帮助。⁷⁵我们应该如何实现这个更好的未来”？

领导这场变革的大部分人仍不为人所知，除了网景公司的创始人马克·安德森这样的老兵外。你应该没有听说过本书中引用的大部分人。不过，其实谁在1994年听说过伊朗移民皮埃尔·奥米戴尔或华尔街程序

员杰夫·贝索斯呢？很多事情取决于产业的领袖们如何介入。区块链会替代脸书（Facebook）或推特（Twitter）吗，或者现有的参与者会通过改善数据所有权和隐私问题来解决用户的担忧吗？这并不重要。无论怎样，消费者都是赢家。Visa会走向失败，还是会通过改变其商业模式去拥抱区块链技术的潜能？苹果会如何应对一个以艺术家为中心的音乐产业？政府官员们会如何面对一个去中心化互联网？区块链技术真的能为世界范围内20亿无法享受银行服务的人提供帮助吗？

初创企业的失败率是很高的，因此我们预计这本书中所研究的很多案例都会失败，这并非因为区块链技术的理念不好，而是对我们所举例的每一个企业来说，都面临着很多也是初创企业的竞争对手。这些初创企业并不可能全部生存下来。我们相信那些追随中本聪的理念的人将会比其他人有着更高的成功率。

这些是充满兴奋和危机的时代。作为一个商业领袖，你可以将《区块链革命》这本书看成是你的行动指南。不过也要意识到游戏规则也在发生变化。你要对你的业务、所做的产业及工作进行思考：我将会被如何影响，我可以做什么？不要重蹈历史上的很多范式转型所遭遇的覆辙。今天的领袖并不能承担成为明日的失败者的风险。这是利害攸关的事情，而我们需要你的帮助。请加入我们。

注释

第一章 可信的协议

[1.https://www.technologyreview.com/s/419452/moores-outlaws/](https://www.technologyreview.com/s/419452/moores-outlaws/).

[2.https://cryptome.org/jya/digicrash.htm](https://cryptome.org/jya/digicrash.htm).

[3.](#)由Ian Grigg和他的同事从荷兰语翻译为英语，并在1999年2月10日发送到Robert Hettinga的邮件列表里；2015年7月19日发表到John Young Architects组织所主办的Cryptome.org网站上；还可以参见<https://cryptome.org/jya/digicash.htm>，及Next! Magazine网站上2015年7月19日的文章“[How DigiCash Alles Verknalde](#)”，网址是www.nextmagazine.nl/ecash.htm；还可以参见<https://web.archive.org/web/19990427/http://nextmagazine.nl/ecash.htm>的历史数据存档。

[4.http://nakamotoinstitute.org/the-god-protocols/](http://nakamotoinstitute.org/the-god-protocols/).

[5.](#)Brian Fung, “Marc Andreessen: In 20 Years, We’ll Talk About Bitcoin Like WeTalk About the Internet Today,” The Washington Post, 2014年5月21日；www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/, 获取于2015年1月21日

[6.](#)对Ben Lawsky的采访, 2015年7月2日。

[7.www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine](http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine).

[8.www.coindesk.com/bitcoin-venture-capital/](http://www.coindesk.com/bitcoin-venture-capital/).

[9.Fung](#), “Marc Andreessen.”

[10.www.coindesk.com/bank-of-england-economist-digital-currency/](http://www.coindesk.com/bank-of-england-economist-digital-currency/).

[11.Leigh Buchanan](#)的一篇题为“American Entrepreneurship Is Actually Vanishing,”的文章, 就Kauffman Foundation的研究作出了报道, 参见www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12.

[12.](#)这个定义是在Don Tapscott and David Ticoll所著的《The Naked Corporation》一书中提出来的(New York: Free Press, 2003).

[13.www.edelman.com/news/trust-institutions-drops-level-great-recession/](http://www.edelman.com/news/trust-institutions-drops-level-great-recession/).

[14.www.gallup.com/poll/1597/confidence-institutions.aspx](http://www.gallup.com/poll/1597/confidence-institutions.aspx).

[15.](#)源自对Carlos Moreira的采访, 2015年9月3日。

[16.](#)Don Tapscott是WiSeKey组织顾问委员会的成员。

[17.](#)有不少作家曾经写过数字时代潜在的黑暗面, Don Tapscott是其中的一员。例子可参见The Digital Economy: Promise and Peril in the Age of Networked Intelligence (New York: McGraw Hill, 1995).

[18.](#)对Carlos Moreira的采访, 2015年9月3日。

[19.](#)Tom Peters, “The Wow Project,” Fast Company, Mansueto Ventures LLC, 1999年4月30日; 参见<http://www.fastcompany.com/36831/wow-project>.

[20.](#)对Carlos Moreira的采访, 2015年9月3日。

[21.](#)“虚拟的你”是一个由Ann Cavoukian和Don Tapscott在这部作品中普及的概念，Who Knows: Safeguarding Your Privacy in a Networked World (New York: McGraw-Hill,1997).

[22.](#)Scott McNealy,Sun Microsystems的首席执行官，他在1999年首次提出这种观点。

[23.](#)对Andreas Antonopoulos的采访, 2015年7月20日。

[24.](#)对Joe Lubin的采访, 2015年7月30日。

[25.](#)最终，复杂的个人数据查询服务将无法读取这些数据，因为这些数据是以加密的形式提供的。不过，这些服务还是可以通过使用同态加密技术而直接将问题提交到加密数据中，从而回答与这些数据有关的问题。

[26.](#)处于前沿的思想家们对除了GDP增长外的繁荣有着更广阔的看法。哈佛大学的Michael Porter已经创建了一个社会进步促进会（social progress imperative），参见<http://www.socialprogressimperative.org>.经济学家Joseph Stiglitz及其他人已经对GDP以外的测量方式进行了研究，参见http://www.insee.fr/fr/publications-et-services/dossiers_web/stiglitz/doc-commission/RAPPORT_anglais.pdf；除此外还有一些尝试通过改善国内因素而提高GDP的探讨，参见<http://www.forbes.com/sites/realspin/2013/11/29/beyond-gdp-get-ready-for-a-new-way-to-measure-the-economy/>.

[27.](#)对Vitalik Buterin的采访,2015年9月30日。

[28.](#)Luigi Marco Bassani, “Life, Liberty and...:Jefferson on Property Rights,”Journal of Libertarian Studies 18(1) (Winter 2004): 58.

[29.](#)对Hernando de Soto的采访,2015年11月27日。

[30.](#)对Hernando de Soto的采访,2015年11月27日。

[31.](#)www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing, 获取于2015年8月12日。

[32.](#)www.inc.com/magazine/201505/leigh-buchanan/the-vanishing-startups-in-decline.html.

[33.](#)Naked City是ABC电视网络于1958年-1963年播出的一部警察题材连续剧。

[34.](#)一篇发表于2015年10月的世界经济论坛报告称这在2027年都不会成为主流。

[35.](#)对David Ticoll的采访,2015年12月12日。

第二章 引导未来：区块链经济七大设计原则

[1.](#)对Ann Cavoukian的采访, 2015年9月2日。

[2.](#)Guy Zyskind, Oz Nathan和Alex “Sandy” Pentland, “Enigma: Decentralized Computation Platform with Guaranteed Privacy,”麻省理工学院2015年的白皮书, 2015年6月10日; 2015年10月3日, arxiv.org/pdf/1506.03471.pdf.

[3.](#)对Ann Cavoukian的采访,2015年9月2日。

[4.](#)对Ann Cavoukian的采访,2015年9月2日。

[5.](#)对Austin Hill的采访, 2015年7月22日。

[6.](#)对Ann Cavoukian的采访, 2015年9月2日。

[7.](#)Vitalik Buterin, “Proof of Stake: How I Learned to Love Weak Subjectivity,”参见以太坊基金会的以太坊博客文章，2014年11月24日；2015年10月3日的网址blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity.

[8.](#)Dino Mark Angaritis, 电子邮件附件，2015年11月27日。他是通过如下方式达成其计算的：假设哈希速率为583,000,000 Gh/s(Gh/s=10亿哈希运算/秒)。在10分钟里有600秒。因此，在十分钟里有 $600 \times 583,000,000 = 349,800,000,000 \times 10$ 亿次的哈希运算。这等于350乘以十的三十次幂，即350,000,000,000,000,000或350百万×百万×10亿。

[9.](#)燃烧量证明（proof of burn）要求矿工将自己的代币发送到一个无法赎回的地址中，而矿工则得到一些可能比自己燃烧掉的价值更高的代币（彩票）。这并不是是一种共识机制，而是一种信任机制。

[10.](#)对Paul Brody的采访，2015年7月7日。

[11.](#)Franklin Delano Roosevelt, “Executive Order 6102—Requiring Gold Coin, Gold Bullion and Gold Certificates to Be Delivered to the Government,” The American Presidency Project, 编辑版。Gerhard Peters和John T.Woolley, 1933年4月5日，www.presidency.ucsb.edu/ws/?pid=14611, 获取于2015年12月2日。

[12.](#)对Josh Fairfield的采访，2015年6月1日。

[13.](#)这提及到了Bandai的数码玩具，其设计目标是让用户照顾及保护好它。如果没有人关怀它，它就会死去。

[14.](#)Joseph E.Stiglitz, “Lessons from the Global Financial Crisis of 2008,” Seoul Journal of Economics 23(3) (2010).

[15.](#)Ernst & Young LLP, “The Big Data Backlash,” 2013年12月，

www.ey.com/UK/en/Services/Specialty-Services/Big-Data-Backlash;
<http://tinyurl.com/ptfm4ax>.

[16.](#)这类攻击是以“女巫”（Sybil）命名的，这名字来源于1973年的一本书上提及的一个被诊断出患有分离性身份识别障碍的妇女，当时所用的假名是Sybil，爱好猫的计算机科学家John “JD”Douceur在一篇2002年的论文中普及了这个词。

[17.](#)Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” www.bitcoin.org, 2008年11月1日；参见www.bitcoin.org/bitcoin.pdf的第六章“Incentive.”

[18.](#)Nick Szabo.“Bit gold.” Unenumerated.Nick Szabo, 2008年12月27日。2015年10月3日，<http://unenumerated.blogspot.com/2005/12/bit-gold.html>.

[19.](#)对Austin Hill的采访,2015年7月22日。

[20.](#)Neal Stephenson, Snow Crash (1992).提及了Snow Crash的虚拟世界，Hiro Protagonist是其中的主角和英雄，Hiro是虚拟世界里的头号黑客。Kongbucks就如比特币那样：franchulate（特许政府，即公司化的国家，源自特许经营franchise和领事馆consulate的结合）可以发行自己的货币。

[21.](#)Ernest Cline, Ready Player One (New York: Crown, 2011).

[22.](#)对Austin Hill的采访, 2015年7月22日。

[23.](#)John Lennon.“Imagine.” Imagine.制作人包括John Lennon、Yoko Ono和Phil Spector, 1971年10月11日面世。参见www.lyrics007.com/John%20Lennon%20Lyrics/Imagine%20Lyrics.html.

[24.](#)Andy Greenberg.“Banking’s Data Security Crisis.” Forbes.2008年11月。2015年3月， www.forbes.com/2008/11/21/data-breaches-cybertheft-identity08-tech-cx_ag_1121breaches.html.

[25.](#)Ponemon Institute LLC, “2015 Cost of Data Breach Study: Global Analysis,”由IBM赞助，2015年5月发布，参见www-03.ibm.com/security/data-breach.

[26.](#)Ponemon Institute LLC, “2014 Fifth Annual Study on Medical Identity Theft,”由Medical Identity Fraud Alliance赞助，2015年2月23日发布，参见Medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft.

[27.](#)对Andreas Antonopoulos的采访，2015年7月20日。

[28.](#)Michael Melone, “Basics and History of PKI,”微软公司Mike Melone的博客，发表于2012年3月10日；可参见2015年10月3日发布的<http://tinyurl.com/ngxuupl>.

[29.](#)“Why Aren’t More People Using Encrypted Email?,”参见Virtru公司的博客，2015年1月24日；www.virtu.com/blog/aren't-people-using-email-encryption, 2015年8月8日。

[30.](#)对Andreas Antonopoulos的采访,2015年7月20日。

[31.](#)对Austin Hill的采访，2015年7月22日。

[32.](#)对Austin Hill的采访，2015年7月22日。

[33.](#)对Ann Cavoukian的采访，2015年9月2日。

[34.](#)对Ann Cavoukian的采访，2015年9月2日。

[35.](#)David McCandless, “Worlds Biggest Data Breaches,” Information Is

Beautiful,David McCandless, 2015年10月2日; 2015年10月3日,
www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[36.](#)对Haluk Kulin的采访, 2015月9日。

[37.](#)对Austin Hill的采访, 2015年7月22日。

[38.](#)Coinbase隐私政策, www.coinbase.com/legal/privacy, 2014年11月17日, 获取于2015年7月15日。

[39.](#)参见Don Tapscott和David Ticoll的The Naked Corporation: How the Age of Transparency Will Revolutionize Business (New York: Simon & Schuster, 2003).

[40.](#)对Haluk Kulin的采访, 2015年6月9日。

[41.](#)参见ProofofExistence.com, 2015年9月2日;
www.proofofexistence.com/about/.

[42.](#)对Steve Omohundro的采访, 2015年5月28日。

[43.](#)对Andreas Antonopoulos的采访, 2015年7月20日。

[44.](#)对Andreas Antonopoulos的采访, 2015年7月20日。

[45.](#)对Stephen Pair的采访, 2015年6月11日。

[46.](#)Edella Schlarger和Elinor Ostrom, “Property-Rights Regimes and Natural Resources: A Conceptual Analysis,” Land Economics 68(3) (August 1992): 249–62;www.jstor.org/stable/3146375.

[47.](#)对Haluk Kulin的采访, 2015年6月9日。

[48.](#)John Paul Titlow, “Fire Your Boss: Holacracy’s Founder on the Flatter Future of Work,” Fast Company, Mansueto Ventures LLC, 2015年7月9日; www.fastcompany.com/3048338/the-future-of-work/fire-your-boss-holacracy-founder-on-the-flatter-future-of-work.

[49.](#)World Bank, 2015年9月2日; www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report.

[50.](#)“Bitcoin Powers New Worldwide Cellphone Top-Up Service,” CoinDesk, 2015年2月15日; www.coindesk.com/bitcoin-powers-new-worldwide-cellphone-top-service/, 获取于2015年8月26日。BitMoby.com问答栏目, mHITs Ltd., n.d.; www.bitmoby.com/faq.html, 获取于2015年11月14日。

[51.](#)对Gavin Andresen的采访, 2015年6月8日。

[52.](#)对Austin Hill的采访, 2015年7月22日

[53.](#)Jakob Nielsen, “Nielsen’s Law of Internet Bandwidth,” Nielsen Norman Group, 1998年4月5日; www.nngroup.com/articles/law-of-bandwidth/, 获取于2015年8月26日。

[54.](#)Matthew Weaver, “World Leaders Pay Tribute at Auschwitz Anniversary Ceremony,” The Guardian, Guardian News and Media Limited, 2015年1月27日; 2015年9月5日, <http://www.theguardian.com/world/2015/jan/27/-sp-watch-the-auschwitz-70th-anniversary-ceremony-unfold>.

第三章 重塑金融服务形象：从赚钱机器变成致富平台

1. [国际货币基金组织预计范围是8750万美元到1.12亿美元。](#)
2. <https://ripple.com/blog/the-true-cost-of-moving-money/>.
3. 对Vikram Pandit的采访，2015年8月24日。
4. www.nytimes.com/2015/07/12/business/mutfund/putting-the-public-back-in-public-finance.html.
5. www.worldbank.org/en/topic/poverty/overview.
6. <http://hbswk.hbs.edu/item/6729.html>.
7. 对Hernando de Soto的采访，2015年11月27日。
8. http://corporate.westernunion.com/About_Us.html.
9. 对Erik Voorhees的采访，2015年6月16日。
10. Paul A. David, “The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox,” *Economic History of Technology* 80(2) (1990年5月): 355–61.
11. Joseph Stiglitz, “Lessons from the Global Financial Crisis,” 这是一个在2009年10月27日于首尔国立大学举办的一个讲座的修改版本。
12. www.finextra.com/finextra-downloads/newsdocs/The%20Fintech%202%200%20Paper.pdf.
13. www.bloomberg.com/news/articles/2015-07-22/the-blockchain-revolution-gets-endorsement-in-wall-street-survey.
14. www.swift.com/assets/swift_com/documents/about_swift/SIF_20150.

- [15.https://lightning.network/](https://lightning.network/).
- [16.](#)对Chris Larsen的采访，2015年7月27日。
- [17.](#)对Austin Hill的采访，2015年7月22日。
- [18.](#)对Blythe Masters的采访，2015年7月27日。
- [19.](#)对Blythe Masters的采访，2015年7月27日。
- [20.](#)对Blythe Masters的采访，2015年7月27日。
- [21.](#)对Blythe Masters的采访，2015年7月27日。
- [22.https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/](https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/).
- [23.](#)对Austin Hill的采访，2015年7月22日。
- [24.](#)Greenwich Associates，2015年7月；参见www.bloomberg.com/news/articles/2015-07-22/the-blockchain-revolution-gets-endorsement-in-wall-street-survey.
- [25.](#)Blythe Masters，在Exponential Finance的主旨演讲，参见www.youtube.com/watch?v=PZ6WR2R1MnM.
- [26.https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/](https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/).
- [27.](#)对Jesse McWaters的采访，August 13, 2015.
- [28.](#)对Austin Hill的采访，July 22, 2015.
- [29.https://blog.ethereum.org/2015/08/07/on-public-and-private-](https://blog.ethereum.org/2015/08/07/on-public-and-private-)

blockchains/.

[30.](#)对Chris Larsen的采访，2015年7月27日。

[31.](#)对Adam Ludwin的采访，2015年7月26日。

[32.](#)对Blythe Masters的采访，2015年7月27日。

[33.](#)对Eric Piscini的采访，2015年7月13日。

[34.](#)对Derek White的采访，2015年7月13日。

[35.](#)对Derek White的采访，2015年7月13日。

[36.](#)此后，Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, SEB, Société Générale及 Toronto Dominion Bank; www.ft.com/intl/cms/s/0/f358ed6c-5ae0-11e5-9846-de406ccb37f2.html#axzz3mf3orbRX; www.coindesk.com/citi-hsbc-partner-with-r3cev-as-blockchain-project-adds-13-banks/.

[37.](#)<http://bitcoinnewsy.com/bitcoin-news-mike-hearn-bitcoin-core-developer-joins-r3cev-with-5-global-banks-including-wells-fargo/>.

[38.](#)<http://www.linuxfoundation.org/news-media/announcements/2015/12/linux-foundation-unites-industry-leaders-advance-blockchain>.

[39.](#)www.ifrasia.com/blockchain-will-make-dodd-frank-obsolete-bankers-say/21216014.article.

[40.](#)<http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnethtml%2FPTO%2Fsearch->

bool.html&r=1&f=G&l=50&co1=AND&d=PG01&s1=20150332395&OS=2(
p=cite_Brian_Cohen_or_Bitcoin_Magazine.

[41.](http://www.youtube.com/watch?v=A6kJfvuNqtg)www.youtube.com/watch?v=A6kJfvuNqtg.

[42.](#)对Jeremy Allaire的采访，2015年6月30日。

[43.](#)对Jeremy Allaire的采访，2015年6月30日。

[44.](#)对Jeremy Allaire的采访，2015年6月30日。

[45.](#)对Jeremy Allaire的采访，2015年6月30日。

[46.](#)被认为这个产业正在“成长”的另一个标志，；
www.wsj.com/articles/goldman-a-lead-investor-in-funding-round-for-bitcoin-
startup-circle-1430363042.

[47.](#)对Jeremy Allaire的采访，2015年6月30日。

[48.](#)对Stephen Pair的采访，2015年6月11日。

[49.](#)Alex Tapscott曾为Vogogo Inc提供咨询服务。

[50.](#)对Suresh Ramamurthi的采访，2015年9月28日。

[51.](#)与Blythe Masters的邮件往来，2015年12月14日。

[52.](#)对Tom Mornini的采访，2015年7月20日。

[53.](#)这些构思最早是在Don Tapscott和David Ticoll所著的The Naked Corporation一书里提出来的。

[54.](#)这些构思最早是在Don Tapscott和David Ticoll所著的The Naked Corporation一书里提出来的。

[55. www.accountingweb.com/aa/auditing/human-errors-the-top-corporate-tax-and-accounting-mistakes.](http://www.accountingweb.com/aa/auditing/human-errors-the-top-corporate-tax-and-accounting-mistakes)

[56. www.accountingweb.com/aa/auditing/human-errors-the-top-corporate-tax-and-accounting-mistakes.](http://www.accountingweb.com/aa/auditing/human-errors-the-top-corporate-tax-and-accounting-mistakes)

[57.](#)对Simon Taylor的采访，2015年7月13日。

[58.](#)对Simon Taylor的采访，2015年7月13日。

[59.](#)对Jeremy Allaire的采访，2015年6月30日。

[60.](#)对Christian Lundkvist的采访，2015年7月6日。

[61.](#)对Austin Hill的采访，2015年7月22日。

[62.](#)对Eric Piscini的采访，2015年7月13日。

[63. www2.deloitte.com/us/en/pages/about-deloitte/articles/facts-and-figures.html.](http://www2.deloitte.com/us/en/pages/about-deloitte/articles/facts-and-figures.html)

[64.](#)对Eric Piscini的采访，2015年7月13日。

[65.](#)对Eric Piscini的采访，2015年7月13日。

[66.](#)对Tom Mornini的采访，2015年7月20日。

[67.](#)对Tom Mornini的采访，2015年7月20日。

[68. www.calpers.ca.gov/docs/forms-publications/global-principles-corporate-governance.pdf.](http://www.calpers.ca.gov/docs/forms-publications/global-principles-corporate-governance.pdf)

[69.](#)对Izabella Kaminska的采访，2015年8月5日。

[70.](http://listedmag.com/2013/06/robert-monks-its-broke-lets-fix-it/)<http://listedmag.com/2013/06/robert-monks-its-broke-lets-fix-it/>.

[71.](#)“被遗忘的权利运动”（The Right to Be Forgotten Movement）正在得到关注，特别是在欧洲：参见http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

[72.](http://www.bloomberg.com/news/articles/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing)www.bloomberg.com/news/articles/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing.

[73.](http://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html)<http://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html>.

[74.](#)对Patrick Deegan的采访，2015年6月6日。

[75.](#)对Patrick Deegan的采访，2015年6月6日。

[76.](https://btcjam.com/)<https://btcjam.com/>.

[77.](#)对Erik Voorhees的采访，2015年7月16日。

[78.](http://www.sec.gov/about/laws/sa33.pdf)www.sec.gov/about/laws/sa33.pdf.

[79.](http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/)<http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/>.

[80.](http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2073583)<http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2073583>.

[81.](https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/)<https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/>.

[82.](#)James Surowiecki, The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business,

Economies, Societies and Nations (New York: Doubleday, 2014).

[83. www.augur.net](http://www.augur.net).

[84.](#)来自于Augur团队的邮件交流记录：核心开发者Jack Peterson和Joey Krug；特殊运作部门Peronet Despeignes.

[85.](#)对Andreas Antonopoulos的采访，2014年12月8日。

[86.](#)对Barry Silbert的采访，2015年9月22日。

[87.](#)对Benjamin Lawsky的采访，2015年7月2日。

第四章 重新设计公司的架构：核心与边缘

[1.](#)对Joe Lubin的采访，2015年7月13日。

[2.](#)像苹果和Spotify这样的公司也可以使用这个新平台，目标是它将会被音乐产业中的很多实体所拥有，特别是艺术家们。如果你创造内容的话，你会比简单地重新售卖别人的内容赚取更多的代币。

[3. https://slack.com/is](https://slack.com/is).

[4. https://github.com](https://github.com).

[5.](#)Coase写道：“企业可以在经济体系中扮演一定的角色，前提是在企业内组织交易的成本小于该交易在市场中执行的成本。当在企业内组织交易的成本超出在市场中执行同样交易的成本后，企业的规模就面临限制。”Oliver Williamson和Sydney G. Winter引用并编辑过，参见The Nature of the Firm (New York and Oxford: Oxford University Press, 1993), 90.

[6.](#)Oliver Williamson, “The Theory of the Firm as Governance Structure:

From Choice to Contract,” The Journal of Economic Perspectives 16(3) (Summer 2002) 171–95.

[7.](#) Oliver Williamson, “The Theory of the Firm as Governance Structure: From Choice to Contract,” The Journal of Economic Perspectives 16(3) (Summer 2002) 171–95.

[8.](#) Peter Thiel与Blake Masters, Zero to One: Notes on Startups, or How to Build the Future (New York: Crown Business, 2014).

[9.](#) Lord Wilberforce, The Law of Restrictive Trade Practices and Monopolies (Sweet & Maxwell, 1966), 22.

[10.](#) 对Yochai Benkler的采访，2015年8月26日。

[11.](#) John Hagel和John Seely Brown, “Embrace the Edge or Perish,” Bloomberg, 2007年11月28日；www.bloomberg.com/bw/stories/2007-11-28/embrace-the-edge-or-perishbusinessweek-business-news-stock-market-and-financial-advice.

[12.](#) 对Vitalik Buterin的采访，2015年9月30日。

[13.](#) 对Andreas Antonopoulos的采访，2015年7月20日。

[14.](#) Way Back Machine是一个例外，它可以让你获得更深入的历史。

[15.](#) Oliver E. Williamson, “The Theory of the Firm as Governance Structure: From Choice to Contract,” Journal of Economic Perspectives 16 (3), Summer 2002.

[16.](#) Oliver E. Williamson, “The Theory of the Firm as Governance Structure: From Choice to Contract,” Journal of Economic Perspectives 16

(3), Summer 2002.

[17.](#)Michael C.Jensen和William H.Meckling, “Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure,” Journal of Financial Economics 305 (1976): 310–11 (认为公司或企业是股东、债权人、管理者或其他人之间的一种自愿关系的集合); 也可以参见, Frank H.Easterbrook和Daniel R.Fischel的The Economic Structure of Corporate Law (Cambridge, Mass.: Harvard University Press, 1991).

[18.](#)Vitalik Buterin, “Bootstrapping a Decentralized Autonomous Corporation: PartI,” Bitcoin Magazine, 2013年9月19日; <https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/>.

[19.](#)Nick Szabo, “Formalizing and Securing Relationships on Public Networks,”<http://szabo.best.vwh.net/formalize.html>.

[20.](#)<http://szabo.best.vwh.net/smart.contracts.html>.

[21.](#)对Aaron Wright的采访, 2015年8月10日。

[22.](#)密码学家们开始使用“Alice”和“Bob”而不是甲方、乙方这类词语, 作为一种描述双方之间交换过程的便利方式, 这样能为计算机加密技术的讨论带来一些明晰性和熟悉性。这样的做法据称源自Ron Rivest在1978年的作品“Security’s Inseparable Couple”, ACM通讯。Network World,2005年2月7日; 参见www.networkworld.com/news/2005/020705widernetaliceandbob.html.

[23.](#)GitHub.com, 2012年1月3日; <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki>, 获取于2015年9月30日

[24.](http://www.coindesk.com/hedgy-hopes-tackle-bitcoin-volatility-using-multi-signature-technolog/)www.coindesk.com/hedgy-hopes-tackle-bitcoin-volatility-using-multi-signature-technolog/.

[25.](https://books.google.ca/books?id=VXIDgGjLHVgC&pg=PA19&lpg=PA19&dq=a+workman+moves+from+JDcAQ6AEIITAB#v=onepage&q=a%20workman%20moves%20from%20de)https://books.google.ca/books?id=VXIDgGjLHVgC&pg=PA19&lpg=PA19&dq=a+workman+moves+from+JDcAQ6AEIITAB#v=onepage&q=a%20workman%20moves%20from%20de

[26.](#)Elliot Jaques, “In Praise of Hierarchy,” Harvard Business Review, 1990年1月-2月刊。

[27.](#)对Yochai Benkler的采访, August 26, 2015.

[28.](#)Tapscott和Ticoll所著的The Naked Corporation一书。

[29.](#)Werner Erhard和Michael C.Jensen, “Putting Integrity into Finance: A Purely Positive Approach,” 2015年11月27日, Harvard Business School NOM Unit Working Paper No.12-074; Barbados Group Working Paper No.12-01; European Corporate Governance Institute (ECGI)—Finance Working Paper No.417/2014.

[30.](#)美国银行自2009年12月31日起平均资本回报率已经低于百分之二; 参见https://ycharts.com/companies/BAC/return_on_equity.

[31.](#)对Steve Omohundro的采访, 2015年5月28日。

[32.](#)对David Ticoll的邮件采访, 2015年9月9日。

[33.](#)对Melanie Swan的采访, 2015年9月14日。

[34.](https://hbr.org/1990/05/the-core-competence-of-the-corporation)https://hbr.org/1990/05/the-core-competence-of-the-corporation.

[35.](#)Michael Porter, “What Is Strategy?,” Harvard Business Review, 1996年11-12月刊。

[36.](#)对Susan Athey的采访，2015年11月20日。

第五章 新商业模式：在区块链上寻找新机会

[1.](#)为防止垃圾信息，可以设计成信用度比较低的新的公钥（身份）需要付出一定的费用才能录入系统中。可以将费用转移到一个担保合约中，当该身份成功地出租了自己的房产，或经历一段时间后他们希望删除所录入的房源，就可以将费用取回来。像图片这样的大型数据文件将会存放在IPFS或Swarm去中心化存储平台上，不过其哈希值和鉴别拥有该数据的身份的信息将会通过区块链保存在bAirbnb的合约上。

[2.](#)或许是使用Whisper协议。

[3.](#)超文本标记语言HTML构建格式和注释。

[4.](#)David McCandless, “World’s Biggest Data Breaches,” Information Is Beautiful,2015年10月2日;
www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, 获取于2015年11月27日。

[5.](#)就如Vitalik Buterin定义的那样，“加密货币经济学是一个技术概念，大约意思是，“它是去中心化的，它使用公钥密码学技术进行验证，并使用经济激励机制去确保它持续运行，其记录不会被回退，也不会出现其他的故障。””参见“The Value of Blockchain Technology,Part I,”
<https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>.

[6.](#)www.youtube.com/watch?v=K2fhwMKk2Eg.

[7.](#)<http://variety.com/2015/digital/news/netflix-bandwidth-usage-internet-traffic-1201507187/>.

[8.](#)对Bram Cohen的采访，2015年8月17日。

[9.](#)Stan Franklin和Art Graesser, “Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents,” www.inf.ufrgs.br/~alvares/CMP124SMA/IsItAnAgentOrJustAProgram.pdf.

[10.](#)Stan Franklin和Art Graesser, “Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents,” www.inf.ufrgs.br/~alvares/CMP124SMA/IsItAnAgentOrJustAProgram.pdf

[11.](#)Vitalik Buterin, <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>.“自主运作的代理人是在自动化的另一个维度；在一个自主运作的代理人中，并不需要特定的人类活动参与；或许说，可能需要有一定的人类活动去建造这些代理人运行所需的硬件，但并不需要有意识到这些代理人存在的人类。”

[12.](#)Vitalik Buterin, <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>.“自主运作的代理人是在自动化的另一个维度；在一个自主运作的代理人中，并不需要特定的人类活动参与；或许说，可能需要有一定的人类活动去建造这些代理人运行所需的硬件，但并不需要有意识到这些代理人存在的人类。”

[13.](#)技术细节：因为在区块链上直接存储数据代价是非常大的，因此更可能是将数据的哈希值保存到区块链上，而数据的内容则存储在去其他去中心化的数据存储网络上，如Swarm或IPFS.

[14.](#)对Vitalik Buterin的采访，2015年9月30日。

[15.](#)对Andreas Antonopoulos的采访，2015年7月20日。

[16.](#)对Andreas Antonopoulos的采访，2015年7月20日。

[17.](#)Don Tapscott和Anthony D.Williams, Wikinomics: How Mass Collaboration Changes Everything (New York: Portfolio/Penguin, 2007).Wikinomics定义了7种这样的商业模式, 在这里对列表进行了展开。

[18.](#)共同对等生产(Commons-based Peer Production)是由哈佛法学院教授Yochai Benkler在一篇题为“Coase’s Penguin”的研讨会文章中提出的, 该文章参见The Yale Law Journal,2002; www.yale.edu/yalelj/112/BenklerWEB.pdf.

[19.](#)<http://fortune.com/2009/07/20/information-wants-to-be-free-and-expensive/>.

[20.](#)对Yochai Benkler的采访, 2015年8月26日。

[21.](#)对Dino Mark Angaritis, 2015年8月7日。

[22.](#)Andrew Lih, “Can Wikipedia Survive?,” The New York Times, 2015年6月20日; www.nytimes.com/2015/06/21/opinion/can-wikipedia-survive.html.

[23.](#)<http://techcrunch.com/2014/05/09/monegraph/>.

[24.](#)<http://techcrunch.com/2015/06/24/ascribe-raises-2-million-to-ensure-you-get-credit-for-your-art/>.

[25.](#)www.nytimes.com/2010/04/15/technology/15twitter.html?_r=0.

[26.](#)<http://techcrunch.com/2014/05/09/monegraph/>.

[27.](#)www.verisart.com/.

[28.](#)<http://techcrunch.com/2015/07/07/verisart-plans-to-use-the->

blockchain-to-verify-the-authencity-of-artworks/.

[29.](#)对Yochai Benkler的采访，2015年8月26日。

[30.](#)对David Ticoll的采访，2015年8月7日。

[31.](#)对Yochai Benkler的采访，2015年8月26日。

[32.](#)www.nytimes.com/2013/07/21/opinion/sunday/friedman-welcome-to-the-sharing-economy.html?pagewanted=1&_r=2&partner=rss&emc=rss&.

[33.](#)Sarah Kessler, “The Sharing Economy Is Dead and We Killed It,” Fast Company, 2015年9月14日；www.fastcompany.com/3050775/the-sharing-economy-is-dead-and-we-killed-it#1.

[34.](#)产消者是Alvin Toffler在Future Shock (1980)里发明的概念；在The Digital Economy (1994) 一书中，Don Tapscott详述了产销合一的概念。

[35.](#)对Robin Chase的采访，2015年9月2日。

[36.](#)<https://news.ycombinator.com/item?id=9437095>.

[37.](#)这个情形最早是由Don Tapscott在下面这个文章里解释的，“The Transparent Burger,” Wired, 2004年3月；http://archive.wired.com/wired/archive/12.03/start.html?pg=2%3ftw=wn_tophead_7.

[38.](#)对Yochai Benkler的采访，2015年8月26日。

[39.](#)在Wikinomics被称为维基工作空间。

[40.](#)CAPTCHA验证码的全称是完全自动化的用于分辨电脑和人类的

公共图灵测试, “Completely Automated Public Turing Test to Tell Computers and Humans Apart.”

[41.](#)对Joe Lubin的采访, 2015年7月13日。

[42.](#)对Joe Lubin的采访, 2015年7月13日。

第六章 万物账本: 物理世界的活化

[1.](#)这并不是他们的真名。这个故事是建立在有着类似情况的人身上的。

[2.](#)Primavera De Filippi, “It’s Time to Take Mesh Networks Seriously (and Not Just for the Reasons You Think),” Wired, 2014年1月2日。

[3.](#)对Eric Jennings的采访, 2015年7月10日。

[4.](#)对Eric Jennings的采访, 2015年7月10日。

[5.](#)对Lawrence Orsini的采访, 2015年7月30日。

[6.](#)Don在Don Tapscott和Anthony Williams的作品中预测了这样的网络的发展, Macrowikinomics: New Solutions for a Connected Planet (New York: Portfolio/Penguin, 2010, 2012年更新)。

[7.](#)对Lawrence Orsini的采访, 2015年7月30日。

[8.](#)Puja Mondal, “What Is Desertification? Desertification: Causes, Effects and Control of Desertification,” UNEP: Desertification, United Nations Environment Programme, n.d.; <https://desertification.wordpress.com/category/ecology-environment/unep/>, 获取于2015年9月29日。

[9.](http://www.internetlivestats.com/internet-users/) www.internetlivestats.com/internet-users/, 截至2015年12月1日。

[10.](#) Cadie Thompson, “Electronic Pills May Be the Future of Medicine,” CNBC, 2013年4月21日; www.cnbc.com/id/100653909; 及Natt Garun, “FDA Approves Edible Electronic Pills That Sense When You Take Your Medication,” Digital Trends, 2012年4月1日; www.digitaltrends.com/home/fda-approves-edible-electronic-pills/.

[11.](#) Mark Jaffe, “IOT Won’t Work Without Artificial Intelligence,” Wired, 2014年11月; www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/.

[12.](#) IBM, “Device Democracy,” 2015, 4.

[13.](#) Allison Arieff, “The Internet of Way Too Many Things,” The New York Times, 2015年9月5日。

[14.](#) IBM, “Device Democracy,” 10.

[15.](#) 对Dino Mark Angaritis的采访, 2015年8月11日。

[16.](#) 对Carlos Moreira的采访, 2015年9月3日。

[17.](#) 对Carlos Moreira的采访, 2015年9月3日。

[18.](#) 对Michelle Tinsley的采访, 2015年6月25日。

[19.](#) 对Michelle Tinsley的采访, 2015年6月25日。

[20.](#) McKinsey Global Institute, “The Internet of Things: Mapping the Value Beyond the Hype,” 2015年6月。

[21.](#) 对Eric Jennings的采访, 2015年7月10日。

[22.](#)IBM Institute for Business Value, “The Economy of Things: Extracting New Value from the Internet of Things,” 2015.

[23.](#)Cadie Thompson, “Apple Has a Smart Home Problem: People Don’t Know They Want It Yet,” Business Insider, 2015年6月4日; www.businessinsider.com/apple-homekit-adoption-2015-6.

[24.](#)McKinsey Global Institute, “The Internet of Things.”

[25.](#)对Eric Jennings的采访，2015年7月10日。

[26.](#)IBM, “Device Democracy,” 9.

[27.](#)IBM, “Device Democracy,” 13.

[28.](#)McKinsey Global Institute, “The Internet of Things.”定义了9种有价值的设定。

[29.](#)www.wikihow.com/Use-Uber.

[30.](#)<http://consumerist.com/tag/uber/page/2/>.

[31.](#)Mike Hearn, “Future of Money,” Turing Festival, Edinburgh, Scotland, 2013年8月23日锁住，2013年9月28日发表；参见 www.youtube.com/watch?v=Pu4PAMFPo5Y&feature=youtu.be.

[32.](#)McKinsey, “An Executive’s Guide to the Internet of Things,” 2015年8月; www.mckinsey.com/Insights/Business_Technology/An_executives_guide_to_cid=digital-eml-alt-mip-mck-oth-1508.

第七章 解决繁荣悖论：经济包容性

- 1.<http://datatopics.worldbank.org/financialinclusion/country/nicaragua>.
- 2.www.budde.com.au/Research/Nicaragua-Telecoms-Mobile-and-Broadband-Market-Insights-and-Statistics.html.
- 3.“Property Disputes in Nicaragua,” U.S.Embassy, http://nicaragua.usembassy.gov/property_disputes_in_nicaragua.html.据估计有30000间房产存在争议。
- 4.对Joyce Kim的采访，2015年6月12日。
- 5.对Joyce Kim的采访，2015年6月12日。
- 6.对Joyce Kim的采访，2015年6月12日。
- 7.www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report; 及C.K.Prahalad, The Fortune at the Bottom of the Pyramid: Eradicating Poverty Through Profits (Philadelphia: Wharton School Publishing, 2009).这个是预计的数字。
- 8.对Joyce Kim的采访，2015年6月12日。
- 9.www.ilo.org/global/topics/youth-employment/lang—en/index.htm.
- 10.Thomas Piketty, Capital in the Twenty-First Century (Cambridge, Mass.: Belknap Press, 2014).
- 11.[www.brookings.edu/~media/research/files/papers/2014/05/declining_business_dynamism_litan/declining_business_dynamism_hathaway_litan.p](http://www.brookings.edu/~media/research/files/papers/2014/05/declining_business_dynamism_litan/declining_business_dynamism_hathaway_litan.pdf)
- 12.Ruth Simon and Caelainn Barr, “Endangered Species: Young U.S.Entrepreneurs,”The Wall Street Journal, 2015年1月2日; www.wsj.com/articles/endangered-species-young-u-s-entrepreneurs-

1420246116.

[13.](#)World Bank Group, Doing Business, www.doingbusiness.org/data/exploretopics/starting-a-business.

[14.](#)对Hernando de Soto的采访，2015年11月27日。

[15.](#)www.tamimi.com/en/magazine/law-update/section-6/june-4/dishonoured-cheques-in-the-uae-a-criminal-law-perspective.html.

[16.](#)www.worldbank.org/en/topic/poverty/overview.精确点说，在1990年是19.1亿。

[17.](#)<http://digitalcommons.georgefox.edu/cgi/viewcontent.cgi?article=1003&context=gfsb>.

[18.](#)<http://reports.weforum.org/outlook-global-agenda-2015/top-10-trends-of-2015/1-deepening-income-inequality/>.

[19.](#)<http://reports.weforum.org/outlook-global-agenda-2015/top-10-trends-of-2015/1-deepening-income-inequality/>.

[20.](#)对Tyler Winklevoss的采访，2015年6月9日。

[21.](#)Congo, Chad, Central African Republic, South Sudan, Niger, Madagascar, Guinea, Cameroon, Burkina Faso, Tanzania; http://data.worldbank.org/indicator/FB.CBK.BRCH.P5?order=wbapi_data_value_2013+wbapi_data_value+wbapi_data_value-last&sort=asc.

[22.](#)www.aba.com/Products/bankcompliance/Documents/SeptOct11Cover

[23.](#)<http://www.nytimes.com/2015/12/24/business/dealbook/banks-reject->

new-york-city-ids-leaving-unbanked-on-sidelines.html.

[24.](#)与Joe Lubin的邮件沟通记录，2015年8月6日。

[25.](#)David Birch, Identity Is the New Money (London: London Publishing Partnership,2014), 1.

[26.](#)与Joe Lubin的邮件沟通记录，2015年8月6日。

[27.](#)对Joyce Kim的采访，2015年6月12日。

[28.](#)对Hernando de Soto的采访，2015年11月27日。

[29.](#)对Haluk Kulin的采访，2015年6月9日。

[30.](#)与Joe Lubin的邮件沟通记录，2015年8月6日。

[31.](#)对Balaji Srinivasan的采访，2014年5月29日。

[32.](http://www.doingbusiness.org/data/exploretopics/starting-a-business)www.doingbusiness.org/data/exploretopics/starting-a-business.

[33.](#)对Haluk Kulin的采访，2015年6月9日。

[34.](#)Analie Domingo同意让我们跟着她，记录她平常向远在菲律宾的母亲汇款的过程。Analie已经是Don Tapscott和Ana Lopes的20年时间的雇员了，也是很亲近的朋友。

[35.](http://www12.statcan.gc.ca/nhs-enm/2011/dp-pd/prof/details/page.cfm?Lang=E&Geo1=PR&Code1=01&Data=Count&SearchText=canada&SearchT)www12.statcan.gc.ca/nhs-enm/2011/dp-pd/prof/details/page.cfm?Lang=E&Geo1=PR&Code1=01&Data=Count&SearchText=canada&SearchT

[36.](https://remittanceprices.worldbank.org/sites/default/files/rpw_report_j)https://remittanceprices.worldbank.org/sites/default/files/rpw_report_j

[37.](#)汇款市场有着5000亿美元的规模；若按照平均7.7%的手续费的话，则是385亿美元的手续费。

[38.](#)Dilip Ratha, “The Impact of Remittances on Economic Growth and Poverty Reduction,” Migration Policy Institute 8 (2013年9月).

[39.](#)Adolf Barajas, 等人, “Do Workers’ Remittances Promote Economic Growth?,”IMF Working Paper, www10.iadb.org/intal/intalcdi/pe/2009/03935.pdf.

[40.](#)“Aid and Remittances from Canada to Select Countries,” Canadian International Development Platform, <http://cidpnsi.ca/blog/portfolio/aid-and-remittances-from-canada/>.

[41.](#)World Bank Remittance Price Index, <https://remittanceprices.worldbank.org/en>.

[42.](#)2011 National Household Survey Highlights, Canadian Census Bureau, www.fin.gov.on.ca/en/economy/demographics/census/nhshi11-1.html.

[43.](#)<https://support.skype.com/en/faq/FA1417/how-much-bandwidth-does-skype-need>.

[44.](#)对Eric Piscini的采访，2015年7月13日。

[45.](#)http://corporate.westernunion.com/Corporate_Fact_Sheet.html.

[46.](#)在行文之时，Abra还没有在加拿大开业。不过，我们在Abra的帮助下成功地通过Analie和她的母亲测试了Abra的技术。

[47.](#)对Bill Barhydt的采访，2015年8月25日。

[48.](#)对Bill Barhydt的采访，2015年8月25日。

[49.](#)对Bill Barhydt的采访，2015年8月25日。

[50.](#)“Foreign Aid and Rent-Seeking, The Journal of International Economics, 2000, 438;<http://conferences.wcfia.harvard.edu/sites/projects.iq.harvard.edu/files/go>

[51.](#)“Foreign Aid and Rent-Seeking, The Journal of International Economics, 2000, 438;<http://conferences.wcfia.harvard.edu/sites/projects.iq.harvard.edu/files/go>

[52.](#)www.propublica.org/article/how-the-red-cross-raised-half-a-billion-dollars-for-haiti-and-built-6-homes.

[53.](#)“Mortality, Crime and Access to Basic Needs Before and After the Haiti Earthquake,”*Medicine, Conflict and Survival* 26(4) (2010).

[54.](#)<http://unicoins.org/>.

[55.](#)Jeffrey Ashe与Kyla Jagger Neilan, 在*Their Own Hands: How Savings Groups Are Revolutionizing Development* (San Francisco: Berrett-Koehler Publishers, 2014)中提及。

[56.](#)E.Kumar Sharma, “Founder Falls,” *Business Today* (India), 2011年12月25日； www.businesstoday.in/magazine/features/vikram-akula-quits-sks-microfiance-loses-or-gains/story/20680.html.

[57.](#)Ning Wang, “Measuring Transaction Costs: An Incomplete Survey,” Ronald Coase Institute Working Papers 2 (2003年2月); www.coase.org/workingpapers/wp-2.pdf.

[58.](#)www.telesurtv.net/english/news/Honduran-Movements-Slam-Repression-of-Campesinos-in-Land-Fight-20150625-0011.html.

[59.](#)USAID, the Millennium Challenge Corporation,及UN Food and

Agriculture Organization.

[60.](#)Paul B.Siegel, Malcolm D.Childress, 及Bradford L.Barham, “Reflections on Twenty Years of Land-Related Development Projects in Central America: Ten Things You Might Not Expect, and Future Directions,” Knowledge for Change Series, International Land Coalition (ILC), Rome, 2013; <http://tinyurl.com/oekhzos>, 访问于2015年8月26日。

[61.](#)Paul B.Siegel, Malcolm D.Childress, 及Bradford L.Barham, “Reflections on Twenty Years of Land-Related Development Projects in Central America: Ten Things You Might Not Expect, and Future Directions,” Knowledge for Change Series, International Land Coalition (ILC), Rome, 2013; <http://tinyurl.com/oekhzos>, 访问于2015年8月26日。

[62.](#)Ambassador Michael B.G.Froman, US Office of the Trade Representative, “2015 National Trade Estimate Report on Foreign Trade Barriers,” USTR.gov, 2015年4月1日; <https://ustr.gov/sites/default/files/files/reports/2015/NTE/2015%20NTE%20H>

[63.](#)对Hernando de Soto的访问，2015年11月27日。

[64.](#)<http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515>.

[65.](#)对Kausik Rajgopal的访问，2015年8月10日。

[66.](#)World Bank, “Doing Business 2015: Going Beyond Efficiencies,” Washington,D.C.: World Bank, 2014; DOI: 10.1596/978-1-4648-0351-2, 版权协议为License Creative Commons Attribution CC BY 3.0 IGO.

[67.](#)“ITU Releases 2014 ICT Figures,” www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VEfalovF_Kg.

[68.](http://www.cdc.gov/healthliteracy/learn/understandingliteracy.html) www.cdc.gov/healthliteracy/learn/understandingliteracy.html.

[69.](http://www.proliteracy.org/the-crisis/adult-literacy-facts) www.proliteracy.org/the-crisis/adult-literacy-facts.

[70.](http://www.cia.gov/library/publications/the-world-factbook/fields/2103.html#136) CIA World Factbook, 识字率统计,
www.cia.gov/library/publications/the-world-factbook/fields/2103.html#136.

第八章 重建政府和民主

[1.](http://europa.eu/about-eu/countries/member-countries/estonia/index_en.htm) http://europa.eu/about-eu/countries/member-countries/estonia/index_en.htm; <http://www.citypopulation.de/Canada-MetroEst.html>.

[2.](#) 在世界经济论坛于阿联酋Abu Dhabi举办的Global Agenda Council会议上（2015年10月），在爱沙尼亚总统Toomas Hendrik Ilves与Don Tapscott之间进行的一场亲身谈话。

[3.](http://www.socialprogressimperative.org/data/spi#data_table/countries/com6,dim1,dim2,dim3,com9,idr35,com6,idr16,idr34) www.socialprogressimperative.org/data/spi#data_table/countries/com6,dim1,dim2,dim3,com9,idr35,com6,idr16,idr34.

[4.](https://e-estonia.com/the-story/the-story-about-estonia/) <https://e-estonia.com/the-story/the-story-about-estonia/>. 爱沙尼亚对其e-Estonia计划非常自豪，并在网上发布了很多信息。在这一章中出现的信息和统计数据都是来自爱沙尼亚政府网站。

[5.](https://e-estonia.com/component/electronic-health-record/) “Electronic Health Record,” e-Estonia.com, n.d.; <https://e-estonia.com/component/electronic-health-record/>, 获取于2015年11月29日。

[6.](https://e-estonia.com/component/e-cabinet/) “e-Cabinet,” e-Estonia.com, n.d.; <https://e-estonia.com/component/e-cabinet/>, 获取于2015年11月29日。

[7.](https://e-estonia.com/component/electronic-land-register/) “Electronic Land Register,” e-Estonia.com, n.d.; <https://e-estonia.com/component/electronic-land-register/>, 获取于2015年11月29日。

[8.](#)Charles Brett, “My Life Under Estonia’s Digital Government,” The Register, www.theregister.co.uk/2015/06/02/estonia/.

[9.](#)对Mike Gault的采访，2015年8月28日。

[10.](#)“Keyless Signature Infrastructure,” e-Estonia.com, n.d.; <https://e-estonia.com/component/keyless-signature-infrastructure/>, 获取于2015年11月29日。

[11.](#)Olga Kharif, “Bitcoin Not Just for Libertarians and Anarchists Anymore,” Bloomberg Business, 2014年10月9日; www.bloomberg.com/bw/articles/2014-10-09/bitcoin-not-just-for-libertarians-and-anarchists-anymore.准确地说，在美国人口中有着很强的自由主义倾向。根据Pew研究中心的数据，有11%的美国人自称是自由主义者，并知道该概念。“In Search of Libertarians,” www.pewresearch.org/fact-tank/2014/08/25/in-search-of-libertarians/.

[12.](#)“Bitcoin Proves the Libertarian Idea of Paradise Would Be Hell on Earth,” Business Insider, www.businessinsider.com/bitcoin-libertarian-paradise-would-be-hell-on-earth-2013-12#ixzz3kQqSap00.

[13.](#)Human Rights Watch, “World Report 2015: Events of 2014,” www.hrw.org/sites/default/files/wr2015_web.pdf.

[14.](#)对Hernando de Soto的采访，2015年11月27日。

[15.](#)Seymour Martin Lipset, Political Man: The Social Bases of Politics, 2nd ed.(London:Heinemann, 1983), 64.

[16.](#)对Hernando de Soto的采访，2015年11月27日。

[17.](#)Hernando de Soto, “The Capitalist Cure for Terrorism,” The Wall

Street Journal,2014年10月10日; www.wsj.com/articles/the-capitalist-cure-for-terrorism-1412973796, 获取于2015年11月27日。

[18.](#)对Hernando de Soto的采访, 2015年11月27日。

[19.](#)对Carlos Moreira的采访, 2015年9月3日。

[20.](#)Melanie Swan, Blockchain: Blueprint for a New Economy (Sebastopol, Calif.: O'ReillyMedia, January 2015), 45.

[21.](#)Emily Spaven, “UK Government Exploring Use of Blockchain Recordkeeping,”CoinDesk, 2015年9月1日; www.coindesk.com/uk-government-exploring-use-of-blockchain-recordkeeping/.

[22.](#)J.P.Buntinx, “‘Blockchain Technology’ Is Bringing Bitcoin to the Mainstream,”Bitcoinist.net, 2015年8月29日; <http://bitcoinist.net/blockchain-technology-bringing-bitcoin-mainstream/>.

[23.](#)Melanie Swan,在Adam Stone中引用, “Unchaining Innovation: Could Bitcoin’sUnderlying Tech Be a Powerful Tool for Government?,”Government Technology,2015年7月10日; www.govtech.com/state/Unchaining-Innovation-Could-Bitcoins-Underlying-Tech-be-a-Powerful-Tool-for-Government.html.

[24.](#)例子参见www.partnerships.org.au/ and www.in-control.org.uk/what-we-do.aspx.

[25.](#)对Perianne Boring的采访, 2015年8月7日; 还可以参见Joseph Young, “8 WaysGovernments Could Use the Blockchain to Achieve ‘Radical Transparency,’”CoinTelegraph, 2015年7月13日; <http://cointelegraph.com/news/114833/8-ways-governments-could-use-the-blockchain-to-achieve-radical-transparency>.

[26.www.data.gov](http://www.data.gov).

[27.www.data.gov.uk](http://www.data.gov.uk).

[28.](#)Ben Schiller, “A Revolution of Outcomes: How Pay-for-Success Contracts Are Changing Public Services,” Co.Exist, www.fastcoexist.com/3047219/a-revolution-of-outcomes-how-pay-for-success-contracts-are-changing-public-services.Also see: www.whitehouse.gov/blog/2013/11/20/building-smarter-more-efficient-government-through-pay-success.

[29.](#)R.C.Porter, “Can You ‘Snowden-Proof’ the NSA?: How the Technology Behind the Digital Currency—Bitcoin—Could Stop the Next Edward Snowden,” Fortuna’s Corner, 2015年6月3日; <http://fortunascorner.com/2015/06/03/can-you-snowden-proof-the-nsa-how-the-technology-behind-the-digital-currency-bitcoin-could-stop-the-next-edward-snowden/>.

[30.](#)Elliot Maras, “London Mayoral Candidate George Galloway Calls for City Government to Use Block Chain for Public Accountability,” Bitcoin News, 2015年7月2日; www.cryptocoinsnews.com/london-mayoral-candidate-george-galloway-calls-city-government-use-block-chain-public-accountability/.

[31.](#)Tapscott, The Digital Economy, 304.

[32.](#)Al Gore, 在We Media会议上的演讲, 2005年10月6日; www.fpp.co.uk/online/05/10/Gore_speech.html.

[33.](#)Al Gore, 在We Media会议上的演讲, 2005年10月6日; www.fpp.co.uk/online/05/10/Gore_speech.html.

[34.](#)“The Persistence of Conspiracy Theories,” The New York Times, 2011年4月30日；

www.nytimes.com/2011/05/01/weekinreview/01conspiracy.html?pagewanted=all&_r=0.

[35.](#)[www.nytimes.com/2014/07/06/upshot/when-beliefs-and-facts-collide.html?mod](http://www.nytimes.com/2014/07/06/upshot/when-beliefs-and-facts-collide.html?module=Search&mabReward=relbias:w;%201RI:6%20%3C{:}%3E)

[ule=Search&mabReward=relbias:w;%201RI:6%20%3C{:}%3E](http://www.nytimes.com/2014/07/06/upshot/when-beliefs-and-facts-collide.html?module=Search&mabReward=relbias:w;%201RI:6%20%3C{:}%3E).

[36.](#)“Plain Language: It’s the Law,” Plain Language Action and Information Network,n.d.: www.plainlanguage.gov/plLaw/, 获取于2015年11月30日。

[37.](#)<https://globalclimateconvergence.org/news/nyt-north-carolinas-election-machine-blunder>.

[38.](#)http://users.encs.concordia.ca/~clark/papers/2012_fc.pdf.

[39.](#)http://link.springer.com/chapter/10.1007%2F978-3-662-46803-6_16.

[40.](#)<http://blogs.wsj.com/digits/2015/07/29/scientists-in-greece-design-cryptographic-e-voting-platform/>.

[41.](#)<http://nvbloc.org/>.

[42.](#)<http://cointelegraph.com/news/114404/true-democracy-worlds-first-political-app-blockchain-party-launches-in-australia>.

[43.](#)www.techinasia.com/southeast-asia-blockchain-technology-bitcoin-insights/.

[44.](#)www.techinasia.com/southeast-asia-blockchain-technology-bitcoin-

insights/.

[45.](http://www.washingtonpost.com/news/wonkblog/wp/2014/08/06/a-comprehensive-investigation-of-voter-impersonation-finds-31-credible-incidents-out-of-one-billion-ballots-cast/)www.washingtonpost.com/news/wonkblog/wp/2014/08/06/a-comprehensive-investigation-of-voter-impersonation-finds-31-credible-incidents-out-of-one-billion-ballots-cast/.

[46.](http://www.eac.gov/research/election_administration_and_voting_survey.as)www.eac.gov/research/election_administration_and_voting_survey.as

[47.](http://america.aljazeera.com/opinions/2015/7/most-americans-dont-vote-in-elections-heres-why.html)http://america.aljazeera.com/opinions/2015/7/most-americans-dont-vote-in-elections-heres-why.html.

[48.](#)对Eduardo Robles Elvira的采访，2015年9月10日。

[49.](http://www.chozabu.net/blog/?p=78)www.chozabu.net/blog/?p=78.

[50.](https://agoravoting.com/)https://agoravoting.com/.

[51.](#)对Eduardo Robles Elvira的采访，2015年9月10日。

[52.](http://cointelegraph.com/news/111599/blockchain_technology_smart_)http://cointelegraph.com/news/111599/blockchain_technology_smart_

[53.](#)David Chaum的专利申请书, “Random Sample Elections,” 2014年6月19日; <http://patents.justia.com/patent/20140172517>.

[54.](https://blog.ethereum.org/2014/08/21/introduction-futarchy/)https://blog.ethereum.org/2014/08/21/introduction-futarchy/.

[55.](#)Federico Ast (@federicoast)和Alejandro Sewrjugin (@asewrjugin), “The CrowdJury, a Crowdsourced Justice System for the Collaboration Era,” <https://medium.com/@federicoast/the-crowdjury-a-crowdsourced-court-system-for-the-collaboration-era-66da002750d8#.e8yynqipo>.

[56.](http://crowdjury.org/en/)http://crowdjury.org/en/.

[57.](#)整个过程在Ast和Sewrjugin的“The CrowdJury”中描述出来了。

[58.](#)在下面的网址中介绍了早期雅典的陪审团选择过程。

www.agathe.gr/democracy/the_jury.html.

[59.](#)在这里可以查看完整的报告和建议，其中包括了世界范围内的模式的描述www.judiciary.gov.uk/reviews/online-dispute-resolution/.

[60.](#)<http://blog.counter-strike.net/index.php/overwatch/>.

[61.](#)Environmental Defense Fund, www.edf.org/climate/how-cap-and-trade-works.

[62.](#)Swan, Blockchain: Blueprint for a New Economy.

[63.](#)对Andreas Antonopoulos的采访，2015年7月20日。

第九章 在区块链上解放文化产业

[1.](#)“2015 Women in Music Honours Announced,” M Online, PRS for Music, 2015年10月22日; www.m-magazine.co.uk/news/2015-women-in-music-honours-announced/, 获取于2015年11月21日;

[2.](#)对Imogen Heap的采访，2015年9月16日。

[3.](#)David Byrne, “The Internet Will Suck All Creative Content Out of the World,”The Guardian, 2014年6月20日; www.theguardian.com/music/2013/oct/11/david-byrne-internet-content-world, 获取于2015年9月20日。

[4.](#)对Imogen Heap的采访, 2015年9月16日。

[5.](#)在Imogen Heap家中，Paul Pacifico和Don Tapscott的对话，2015年

11月8日。

[6.](#)“Hide and Seek,”由Ariana Grand演绎, YouTube, Love Ariana Grande Channel, 2015年10月17日; www.youtube.com/watch?v=2SDVDd2VpP0, 获取于2015年11月21日。

[7.](#)对Imogen Heap的采访, 2015年9月16日。

[8.](#)David Byrne等人, “Once in a Lifetime,” Remain in Light, Talking Heads, 1981年2月2日。

[9.](#)对Imogen Heap的采访, 2015年9月16日。

[10.](#)Johan Nylander, “Record Labels Part Owner of Spotify,” The Swedish Wire, 日期未知;www.swedishwire.com/jobs/680-record-labels-part-owner-of-spotify, 获取于2015年9月23日。根据Nylander的资料, Sony有5.8%, Universal有4.8%, Warner有3.8%。在出售之前, EMI有1.9%的股份。

[11.](#)对Imogen Heap的采访, 2015年9月16日。

[12.](#)David Johnson, “See How Much Every Top Artist Makes on Spotify,” Time, 2014年11月18日; <http://time.com/3590670/spotify-calculator/>, 获取于2015年9月25日。

[13.](#)Micah Singleton, “This Was Sony Music’s Contract with Spotify,” The Verge, 2015年5月19日; www.theverge.com/2015/5/19/8621581/sony-music-spotify-contract, 获取于2015年9月25日。

[14.](#)Stuart Dredge, “Streaming Music: What Next for Apple, YouTube, Spotify ...and Musicians?,” The Guardian, 2014年8月29日; www.theguardian.com/technology/2014/aug/29/streaming-music-apple-

youtube-spotify-musicians, 获取于2015年8月14日。

[15.](#)Ed Christman, “Universal Music Publishing’s Royalty Portal Now Allows Writers to Request Advance,” Billboard, 2015年7月20日; www.billboard.com/articles/business/6634741/universal-music-publishing-royalty-window-updates, 获取于2015年11月24日。

[16.](#)Robert Levine, “Data Mining the Digital Gold Rush: Four Companies That Get It,” Billboard 127(10) (2015): 14–15.

[17.](#)对Imogen Heap的采访, 2015年9月16日。

[18.](#)Imogen Heap, “Panel Session,” Guardian Live, “Live Stream: Imogen Heap Releases Tiny Human Using Blockchain Technology, Sonos Studio London,” 2015年10月2日; www.theguardian.com/membership/2015/oct/02/live-stream-imogen-heap-releases-tiny-human-using-blockchain-technology.由ImogenHeap编辑的文章, 电子邮件, 2015年11月27日。

[19.](#)Imogen Heap, “Panel Session,” Guardian Live, “Live Stream: Imogen Heap Releases Tiny Human Using Blockchain Technology, Sonos Studio London,” 2015年10月2日; www.theguardian.com/membership/2015/oct/02/live-stream-imogen-heap-releases-tiny-human-using-blockchain-technology.由ImogenHeap编辑的文章, 电子邮件, 2015年11月27日。

[20.](#)对Andreas Antonopoulos的采访, 2015年7月20日。

[21.](#)对Imogen Heap的采访, 2015年9月16日。

[22.](#)对Imogen Heap的采访, 2015年9月16日。

[23.](#)Stuart Dredge, “How Spotify and Its Digital Music Rivals Can Win Over Artists:‘Just Include Us,’” The Guardian,2013年10月29日;
www.theguardian.com/technology/2013/oct/29/spotify-amanda-palmer-songkick-vevo,获取于2015年8月14日。

[24.](#)George Howard, “Bitcoin and the Arts: 对艺术家及作曲家Zoe Keating的采访, Forbes,2015年6月5日;
www.forbes.com/sites/georgehoward/2015/06/05/bitcoin-and-the-arts-and-interview-with-artist-and-composer-zoe-keating/, 获取于2015年8月14日。

[25.](#)George Howard, “Bitcoin and the Arts: 对艺术家及作曲家Zoe Keating的采访, Forbes,2015年6月5日;
www.forbes.com/sites/georgehoward/2015/06/05/bitcoin-and-the-arts-and-interview-with-artist-and-composer-zoe-keating/, 获取于2015年8月14日。

[26.](#)Joseph Young, “Music Copyrights Stored on the Bitcoin BlockChain: Rock Band22HERTZ Leads the Way,” CoinTelegraph, 2015年5月6日;
<http://cointelegraph.com/news/114172/music-copyrights-stored-on-the-bitcoin-blockchain-rock-band-22hertz-leads-the-way>, 获取于2015年8月14日。

[27.](#)媒体通告, “Colu Announces Beta Launch and Collaboration with Revelator to Bring Blockchain Technology to the Music Industry,” Business Wire, 2015年8月12日。

[28.](#)Gideon Gottfried, “How ‘the Blockchain’ Could Actually Change the Music Industry, Billboard, August 5, 2015;
www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry.

[29.](#)PeerTracks Inc., 2015年9月24日; <http://peertracks.com/>.

[30.](#)“About Us,” Artlery: Modern Art Appreciation, 2015年9月3日;
<https://artlery.com>.

[31.](#)Mark Henricks, “The Billionaire Dropout Club,” CBS MarketWatch, CBS Interactive Inc., 2011年1月24日, 于2011年1月26日更新;
www.cbsnews.com/news/the-billionaire-dropout-club/, 获取于2015年9月20日。

[32.](#)对Joichi Ito的采访, 2015年8月24日。

[33.](#)对Joichi Ito的采访, 2015年8月24日。

[34.](#)对Melanie Swan的采访, 2015年9月14日。

[35.](#)对Melanie Swan的采访, 2015年9月14日。

[36.](#)“Introducing UNESCO: What We Are.”获取于2015年11月28日;
<http://www.unesco.org/new/en/unesco/about-us/who-we-are/introducing-unesco>.

第十章 克服困难：实施过程中的**10**个挑战

[1.](#)Lev Sergeyevich Termen, “Erhöhung der Sinneswahrnehmung durch Hypnose[Increase of Sense Perception Through Hypnosis],” Erinnerungen an A.F.Joffe,1970.“Theremin, Léon,” Encyclopedia of World Biography, 2005, Encyclopedia.com,www.encyclopedia.com, 获取于2015年8月26日。

[2.](#)Maciej Ceglowski, “Our Comrade the Electron,” Webstock 2014上的演讲; St.James Theatre, Wellington, New Zealand, 2014年2月14日;
www.webstock.org.nz/talks/our-comrade-the-electron/, 获取于2015年8月26日。Ceglowski的讨论启发了这一章的开头部分。

[3.](#)对Andreas Antonopoulos的采访，2015年7月20日。

[4.](#)对Tyler Winklevoss的采访，2015年6月9日。

[5.](#)Satoshi Nakamoto, P2pfoundation.ning.com, 2009年2月18日。

[6.](#)Ken Griffith和Ian Grigg, “Bitcoin Verification Latency: The Achilles Heel for Time Sensitive Transactions,”白皮书，2014年2月3日；<http://iang.org/papers/BitcoinLatency.pdf>, 获取于2015年7月20日。

[7.](#)对Izabella Kaminska的采访，2015年8月5日。

[8.](#)对Izabella Kaminska的采访，2015年8月5日。

[9.](#)Primavera De Filippi和Aaron Wright, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia,” Social Sciences Research Network, 2015年3月10日, 43.

[10.](#)对Josh Fairfield的采访，2015年6月1日。

[11.](#)Izabella Kaminska, “Bitcoin’s Wasted Power—and How It Could Be Used to Heat Homes,” FT Alphaville, Financial Times, 2014年9月5日。

[12.](#)CIA, “The World Factbook,” www.cia.gov, 2012; <http://tinyurl.com/noxwvle>, 获取于2015年8月28日。注意塞浦路斯在同期的碳排放为880.1万兆吨（2012年）。

[13.](#)“After the Bitcoin Gold Rush,” The New Republic, 2015年2月24日；www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boombust-cycle, 获取于2015年5月15日。

[14.](#)对Bob Tapscott的采访，2015年7月28日。

- [15.](#)对Gavin Andresen的采访，2015年6月8日。
- [16.](#)对Eric Jennings的采访，2015年7月10日。
- [17.](#)对Stephen Pair的采访，2015年6月11日。
- [18.](#)对Erik Voorhees的采访，2015年6月16日。
- [19.](#)Sangjin Han, “On Fair Comparison Between CPU and GPU,”博客，2013年2月12日； www.eecs.berkeley.edu/~sangjin/2013/02/12/CPU-GPU-comparison.html,获取于2015年8月28日。
- [20.](#)对Bob Tapscott的采访，2015年7月28日。
- [21.](#)对Valery Vavilov的采访，2015年7月24日。
- [22.](#)Hass McCook, “Under the Microscope: Economic and Environmental Costs of Bitcoin Mining,” CoinDesk Ltd., 2014年6月12日； www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/,获取于2015年8月28日。
- [23.](#)对Bob Tapscott的采访，2015年7月28日。
- [24.](#)my-mr-wanky, eBay.com, 2014年5月8日； www.ebay.com/itm/3-Cointerra-Terra-Miner-IV-Bitcoin-Miner-1-6-TH-s-ASIC-Working-Units-in-Hand-/331192098368,获取于2015年7月25日。
- [25.](#)“PC Recycling,” MRI of Australia, MRI (Aust) Pty Ltd.2015年8月28日； <http://www.mri.com.au/pc-recycling.shtml>.
- [26.](#)对Gavin Andresen的采访，2015年6月8日。
- [27.](#)Vitalik Buterin, “Proof of Stake: How I Learned to Love Weak

Subjectivity,”以太坊博客，2014年11月25日；
<https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>.

[28.](#) Stefan Thomas和Evan Schwartz, “Ripple Labs’ W3C Web Payments,”意见书，2014年3月18日；
www.w3.org/2013/10/payments/papers/webpayments2014-submission_25.pdf.

[29.](#)对Austin Hill的采访，2015年7月22日。

[30.](#)对Roger Ver的采访，2015年4月30日。

[31.](#) Satoshi Nakamoto, “Re: Bitcoin P2P E-cash Paper,” The Mail Archive, 2008年11月7日；www.mail-archive.com/,
<http://tinyurl.com/oofvok7>, 获取于2015年7月13日。

[32.](#)对Josh Fairfield的采访，2015年6月1日。

[33.](#)对Stephen Pair的采访，2015年6月11日。

[34.](#)对Jerry Brito的采访，2015年6月29日。

[35.](#)对Jerry Brito的采访，2015年6月29日。

[36.](#)对Josh Fairfield的采访，2015年6月1日

[37.](#)对Andreas Antonopoulos的采访，2015年6月20日。

[38.](#)对Izabella Kaminska的采访，2015年8月5日。

[39.](#)对Stephen Pair的采访，2015年6月11日。

[40.](#)Andrew Vegetabile, “An Objective Look into the Impacts of Forking Blockchains Due to Malicious Actors,” The Digital Currency Council, 2015年7月9日; www.digitalcurrencycouncil.com/professional/an-objective-look-into-the-impacts-of-forking-blockchains-due-to-malicious-actors/.

[41.](#)对Keonne Rodriguez的采访, 2015年5月11日。

[42.](#)Vegetabile, “An Objective Look.”

[43.](#)Peter Todd, “Re: [Bitcoin-development] Fwd: Block Size Increase Requirements,”The Mail Archive, 2015年6月1日; www.mail-archive.com/http://tinyurl.com/pk4ordw, 获取于2015年8月26日。

[44.](#)Satoshi Nakamoto, “Re: Bitcoin P2P E-cash Paper,”邮件列表, 密码学, Metzger, Dowdeswell & Co.LLC, 2008年11月11日。2015年7月13日, www.metzdowd.com/mailman/listinfo/cryptography.

[45.](#)Pascal Bouvier, “Distributed Ledgers Part I: Bitcoin Is Dead,” FiniCulture博客, 2015年8月4日; 获取于2015年8月28日。

[46.](#)Western Union, “Company Facts,” Western Union, Western Union Holdings,Inc., 2014年12月31日; 2016年1月13日; http://corporate.westernunion.com/Corporate_Fact_Sheet.html.

[47.](#)对Gavin Andresen的采访, 2015年6月8日。

[48.](#)对Gavin Andresen的采访, 2015年6月8日。

[49.](#)对Austin Hill的采访, July 22, 2015.

[50.](#)对Gavin Andresen的采访, 2015年6月8日。

[51.](#)Andreas Antonopoulos, “Bitcoin as a Distributed Consensus Platform

and the Blockchain as a Ledger of Consensus States,”对Andreas Antonopoulos的采访，2014年12月9日。

[52.](#)Andy Greenberg, “Hackers Remotely Kill a Jeep on the Highway— with Me in It,” Wired, 2015年7月21日。

[53.](#)International Joint Conference on Artificial Intelligence, 2015年7月28日, Buenos Aires, Argentina; http://futureoflife.org/AI/open_letter_autonomous_weapons#signatories.

[54.](#)Lisa Singh, “Father of the Internet Vint Cerf’s Forecast for ‘Internet of Things,’”Washington Exec, 2015年8月17日。

[55.](#)对Keonne Rodriguez的采访，2015年5月11日。

[56.](#)Cegłowski, “Our Comrade the Electron.”

[57.](#)对Ann Cavoukian的采访，2015年9月2日。

[58.](#)Cegłowski, “Our Comrade the Electron.”

[59.](#)<http://www.lightspeedmagazine.com/nonfiction/interview-marc-goodman/>.

[60.](#)Marc Goodman, Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It (New York, Doubleday, 2015).

[61.](#)对Steve Omohundro的采访，2015年5月28日。

[62.](#)The Silver Stallion, 第26章; www.cadaeic.net/cabell.htm, 获取于2015年10月2日。

[63.](#)对Yochai Benkler的采访，2015年8月26日。

第十一章 下一代的领导者

[1.](#)Stephan Tual, “Announcing the New Foundation Board and Executive Director,”以太坊博客，以太坊基金会，2015年7月30日；
<https://blog.ethereum.org/2015/07/30/announcing-new-foundation-board-executive-director/>, 获取于2015年12月1日。

[2.](#)Ethereum: The World Computer, produced by Ethereum, YouTube, 2015年7月30日； www.youtube.com/watch?v=j23HnORQXvs, 获取于2015年12月1日。

[3.](#)对Vitalik Buterin的采访，2015年9月30日。

[4.](#)对Vitalik Buterin的采访，2015年9月30日。

[5.](#)对Vitalik Buterin的采访，2015年9月30日。

[6.](#)对Vitalik Buterin的采访，2015年9月30日。

[7.](#)Henry VI, part 2, act 4, scene 2.

[8.](#)与Vitalik Buterin的邮件交流，2015年10月1日。

[9.](#)David D.Clark, “A Cloudy Crystal Ball,”展示, IETF, 1992年7月16日； http://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf.

[10.](#)对Brian Forde的采访，2015年6月26日。

[11.](#)对Erik Voorhees的采访，2015年6月16日。对Andreas Antonopolous的采访，2015年6月20日。

[12.](#)对Erik Voorhees的采访，2015年6月16日。

- [13.](#)对Jim Orlando的采访，2015年9月28日。
- [14.](http://www.coindesk.com/bitcoin-venture-capital/)<http://www.coindesk.com/bitcoin-venture-capital/>。
- [15.](#)与Tim Draper的邮件往来记录，2015年8月3日。
- [16.](#)对Gavin Andresen的采访，2015年6月8日。
- [17.](#)对Gavin Andresen的采访，2015年6月8日。
- [18.](#)对Brian Forde的采访，2015年6月26日。
- [19.](#)对Joichi Ito的采访，2015年8月24日。
- [20.](#)对Jerry Brito的采访，2015年6月29日。
- [21.](#)对Jerry Brito的采访，2015年6月29日。
- [22.](http://www.cryptocoinsnews.com/us-colleges-universities-offering-bitcoin-courses-fall/)www.cryptocoinsnews.com/us-colleges-universities-offering-bitcoin-courses-fall/。
- [23.](#)对Adam Draper的采访，2015年5月31日。
- [24.](#)对Benjamin Lawsky的采访，2015年7月2日。
- [25.](#)在Money 2020会议上对Perianne Boring的采访，2015年10月26日。
- [26.](#)对Joichi Ito的采访，2015年8月24日。
- [27.](#)对Blythe Masters的采访，2015年7月29日。
- [28.](#)若要查看Lawsky在担任NYDFS负责人时取得的主要成绩的完整列表，请访问www.dfs.ny.gov/reportpub/2014_annualrep_summ_mea.htm。

[29.](#)对Benjamin Lawsky的采访，2015年7月2日。

[30.](#)对Benjamin Lawsky的采访，2015年7月2日。

[31.](#)对Benjamin Lawsky的采访，2015年7月2日。

[32.](#)对Jerry Brito的采访，2015年6月29日。

[33.](#)对Benjamin Lawsky的采访，2015年7月2日。

[34.](#)对Benjamin Lawsky的采访，2015年7月2日。

[35.](#)若有人要寻找一个传统的保守政府机构所提出的新看法，就要阅读面这个网址的内容了，

www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf.

[36.](#)若有人要寻找一个传统的保守政府机构所提出的新看法，就要阅读面这个网址的内容了，

www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf.

[37.](#)对加拿大参议员Doug Black的采访，2015年7月8日。

[38.](#)对加拿大参议员Doug Black的采访，2015年7月8日。

[39.](#)对加拿大参议员Doug Black的采访，2015年7月8日。

[40.](#)对加拿大参议员Doug Black的采访，2015年7月8日。

[41.](#)对加拿大参议员Doug Black的采访，2015年7月8日。

[42.](#)对Aaron Wright的采访，2015年8月10日。

[43.](#)对Josh Fairfield的采访，2015年6月1日。

[44.](#)美国联邦储备银行并非美国首个国家银行。第一国家银行是由国会于1791年创建出来的，并由美国首个财政部长Alexander Hamilton设计其架构，其规模受到很大的限制，Andrew Jackson总统最终在1836年解散了第一国家银行的继任者第二国家银行。

[45.](#)对Carolyn Wilkins的采访，2015年8月27日。

[46.](#)<http://qz.com/148399/ben-bernanke-bitcoin-may-hold-long-term-promise/>.

[47.](#)在加拿大：
www.bankofcanada.ca/wpcontent/uploads/2010/11/regulation_canadian_financial_innovation_in_the_us.pdf
在美国：www.federalreserve.gov/pf/pdf/pf_5.pdf.

[48.](#)对Carolyn Wilkins的采访，2015年8月27日。

[49.](#)“Money in a Digital World,” Carolyn Wilkins的评论,加拿大央行高级副行长，Wilfred Laurier University, Waterloo, Ontario,2014年11月13日。

[50.](#)对Carolyn Wilkins的采访，2015年8月27日。

[51.](#)对Carolyn Wilkins的采访，2015年8月27日。

[52.](#)对Jerry Brito的采访，2015年6月29日。

[53.](#)对Steve Beauregard的采访，2015年4月30日。

[54.](#)对Jerry Brito的采访，2015年6月29日。

[55.](#)Don Tapscott及Lynne St.Amour, “The Remarkable Internet Governance Network—Part I,” Global Solution Networks Program, Martin Prosperity Institute,University of Toronto, 2014.

[56.](#)与Vint Cerf的邮件记录，2015年6月12日。

[57.](#)www.w3.org/Payments/.

[58.](#)www.intgovforum.org/cms/wks2015/index.php/proposal/view_public

[59.](#)www.internetsociety.org/inet-bangkok/speakers/mr-pindar-wong.

[60.](#)Adam Killick, “Knowledge Networks,” Global Solution Networks Program, Martin Prosperity Institute, University of Toronto, 2014.

[61.](#)对Jerry Brito的采访，2015年6月29日。

[62.](#)对Tyler Winklevoss的采访，2015年6月9日。

[63.](#)对Joichi Ito的采访，2015年8月24日。

[64.](#)http://coala.global/?page_id=13396.

[65.](#)www.digitalchamber.org/.

[66.](#)<https://blog.coinbase.com/2014/10/13/welcome-john-collins-to-coinbase/>.

[67.](#)<http://www.digitalchamber.org/assets/press-release-g7-for-website.pdf>.

[68.](#)Anthony Williams, “Platforms for Global Problem Solving,” Global Solution Networks Program, Martin Prosperity Institute, University of Toronto 2013.

[69.](#)对Brian Forde的采访，2015年6月26日。

[70.](#)对Gavin Andresen的采访，2015年6月8日。

[71. www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Poi](http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Poi)
7.

[72.](#)对Constance Choi的采访，2015年4月10日。

[73.](#)数字化革命已经进入了棋局的下半场，这是由美国发明家及作者Ray Kurzweil所创的一个精明词汇。他讲述了一个故事，有个国王对下棋相当感兴趣，他为这个游戏的发明者提供其想要的任何奖励。发明者要求用大米作为回报。“我想在棋盘的第一格获得1颗大米，在第二格获得2颗大米，第三格获得4颗大米，如此类推，直到最后一格”，他说道。国王想，这加起来最多就一袋大米而已，于是高兴地同意了。国王被误导了。虽然开始时需要的大米数量很少，但在数到棋盘中间的时候，所需的大米数量已经超过20亿颗了。最终需要的数量是9亿亿颗大米，这足以覆盖整个地球了。

[74.](#)对Timothy Draper的电子邮件采访，2015年8月3日。

[75.](#)对Hernando de Soto的采访，2015年11月27日。

附录

区块链专业术语表

51% attack 51%攻击

alt-coin 替代性货币

arbitrary-state 任意状态

Autonomous Agent 自主运作的代理人

Autonomous Vehicle 无人驾驶汽车

Bitcoin 比特币

block 区块

block size 区块尺寸

blockchain 区块链

Consensus Algorithm 共识算法

crypto-currency 加密货币

Dapps 去中心化应用程序

decentralized 去中心化

distributed 分布式

Distributed Ledger Technology 分布式账本技术

Double Spending 双重支付

Ethereum 以太坊

fork 分叉

hash 哈希

hashing power 算力（哈希运算能力）

hierarchical 层级化的（阶层化的）

holacracy 全体共治

inclusion 包容性（普惠）

Internet of Things 物联网

ledger 账本

Ledger of Everything 万物账本

miner 矿工

mining 挖矿

mining machine 矿机

mining pool 矿池

Peer to Peer 点对点

Personal Avatar 个人化身

Private Key 私钥

Proof-of-Stake 权益证明机制

Proof-of-Work 工作量证明

protocol 协议

Public Key 公钥

Satoshi Nakamoto 中本聪

Smart Contract 智能合约

sybil attack 女巫攻击（冒名攻击）

Turing complete 图灵完备

World Wide Web 万维网

出版声明

区块链技术作为新兴技术会对社会的发展产生深远影响。我社出版《区块链革命》旨在帮助读者正确认识区块链技术，知晓其应用也具有“双刃剑”效益，从而帮助人们在运用这种技术时，做到趋利避害。此外，中国人民银行等五部委联合发布的银发【2013】289号文件规定：比特币应当是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。

本社郑重声明：《区块链革命》书中的观点与内容不代表我社的立场和观点。读者若依据本书，做出决策，均与我社无关。

中信出版集团

图书在版编目 (CIP) 数据

区块链革命：比特币底层技术如何改变货币、商业和世界 / (加) 唐塔普斯科特, (加) 亚力克斯·塔普斯科特著；凯尔, 孙铭, 周沁园译. --北京：中信出版社，2016.10

书名原文: Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the world

ISBN 978-7-5086-6685-3

I. ①区... II. ①唐... ②亚... ③凯... ④孙... ⑤周... III. ①电子货币—研究 IV. ①F830.46

中国版本图书馆CIP数据核字 (2016) 第217336号

区块链革命：比特币底层技术如何改变货币、商业和世界

著者：[加] 唐塔普斯科特 [加] 亚力克斯·塔普斯科特

译者：凯尔 孙铭 周沁园

策划推广：中信出版社 (China CITIC Press)

出版发行：中信出版集团股份有限公司

(北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029)

(CITIC Publishing Group)

电子书排版：张明霞

中信出版社官网：<http://www.citicpub.com/>

官方微博：<http://weibo.com/citicpub>

更多好书，尽在中信书院

中信书院：App下载地址<https://book.yunpub.cn/> (中信官方数字阅读平台)

微信号：中信书院

万向区块链实验室丛书

BLOCKCHAIN SOCIETY

DECODING GLOBAL BLOCKCHAIN APPLICATION
AND INVESTMENT CASES

区块链社会

解码区块链全球应用与投资案例

龚鸣（暴走恭亲王）◎著

独家披露258个区块链行业内投融资案例详细数据

拥抱颠覆，区块链社会的商业投资指南

区块链铅笔创始人龚鸣暴走恭亲王全新力作



中信出版社 CHINACITYPRESS

区块链社会：解码区块链全球应用与投资案例

龚鸣 著

中信出版社

目录

序一 链接金融 链接未来

序二 区块链的研究与应用并重

序三 区块链：数字另类资产的新大陆

前言

第一章 区块链：信任的机器

- 一、为什么会出现区块链
- 二、“价值转移”的本质
- 三、什么是区块链
- 四、比特币的底层技术
- 五、区块链的模型架构
- 六、区块链的共识机制
- 七、区块链的类型
- 八、区块链的发展脉络

第二章 智能合约

- 一、什么是智能合约
- 二、智能合约的三要素
- 三、智能合约的范例
- 四、智能合约的应用案例

五、智能合约可能面临的威胁

六、智能合约的未来展望

第三章 DAO和DAC

一、关于DAO和DAC

二、燃料货币理论

第四章 区块链项目介绍

一、区块链项目的基础架构

二、支付汇款

三、数字货币交易所

四、去中心化交易所

五、去中心化电子商务

六、公证和鉴证服务

七、开发平台

八、物联网和供应链

九、智能合约

十、存储与下一代互联网

十一、其他领域

第五章 区块链在非金融行业的应用

一、区块链+医疗行业

二、区块链+保险行业

三、区块链+能源行业

第六章 传统金融行业的区块链战略

- 一、银行的区块链战略
- 二、金融和IT巨头的区块链战略
- 三、咨询巨头的区块链案例分析
- 四、证券交易所的区块链案例分析

第七章 全球区块链投融资分析

- 一、主要的投资领域
- 二、不同地区/国家的投资差异
- 三、不同年度的投资重点差异
- 四、ICO方式的崛起
- 五、总结

第八章 各国对区块链的法律监管情况

- 一、各国政府或地区如何监管数字货币与区块链
- 二、全球证券监管

第九章 区块链重塑世界

- 一、快速变化的开始
- 二、程序设计理念的变化
- 三、数据库进入全新阶段
- 四、金融互联网的出现
- 五、资产证券化的加速
- 六、资产发行方式的巨变
- 七、人类首次大规模协作的开始
- 八、颠覆现代商业社会

版权页

序一 链接金融 链接未来

李礼辉^[1]

最近两年，“区块链”迅速成为技术创新的热词。区块链技术应用得到越来越多的关注。国际货币基金组织（IMF）在首份数字货币报告中指出，区块链“具有改变金融的潜力”；英国政府发行的《分布式账本技术：超越区块链》提出，将优先在传统金融行业应用区块链技术；纳斯达克借助区块链建立私人股权交易平台Linq；花旗、汇丰、富国等银行加入R3区块链联盟并设置自己的研究实验室，德勤借助基于区块链的Rubix平台提供咨询和审计。在我国，中国平安加入R3，万向成立区块链实验室，中国互联网金融协会成立区块链研究工作组。区块链是否如同互联网一样，将会改变金融、改变生活方式、改变商业模式？这是人们正在思考和探索的课题。

区块链最早作为比特币的技术应用，起源于2008年。经过不断的迭代演进，区块链形成分布式（Decentralized）、免信任（Trustless）、时间戳（Time Stamp）、非对称加密（Asymmetric Cryptography）和智能合约（Smart Contract）等五大技术特征。进一步探讨，我们发现，区块链应该是一种更加切合市场经济和现代生活方式需求的应用技术。

首先，区块链的智能合约功能，可以应用于契约关系和契约原则的维护和执行。契约精神是市场经济社会的支柱，体现契约精神的契约关系和契约原则，以及上升到公法领域的公权力，对于建立良好秩序、保障市场经济健康运行具有基础性的意义。在市场经济社会中，契约原则一般是通过良俗的推行、法律的实施、合约的履行来实现的。良俗是约定俗成的文明理念和行为准则，法律是写在纸上的规则，合约既有白纸

黑字的约定也有口头的承诺。这就存在一个可能被利用的“缝隙”：违背良俗、冒犯法律、背离合约的行为有时难以在实施的过程中被及时制止和纠正。

例如，票据是便捷的支付结算工具和融资工具，也是中央银行重要的货币政策工具。2015年，我国累计签发商业汇票22.4万亿元，比2001年增长17倍，金融机构累计贴现102.1万亿元，比2001年增长56倍。而现行票据业务存在的缺陷，主要在于难以有效管控和防范操作性风险和道德风险，包括贸易背景造假，票据真实性认证失效，“一票多卖”，利用票据违规融资套利等等。票据业务监管只能通过现场审核的方式进行，缺乏全流程快速调阅和审查的手段，监管效率低、成本高。如果应用区块链技术构建数字票据，就有可能通过可编程的智能合约形式，实现商业约定的具体限制，引入监管控制节点，由交易各方确认交易，确保价值交换的唯一性。

其次，区块链的分布式、时间戳和非对称加密功能，可以应用于信息的查询、验证和保护。现代社会产生的信息是海量的、几何级增长的。信息大致可以区分为共享信息、专有信息、私密信息。共享信息的价值在于真实，必须维护其权威性；专有信息的价值在于归属，必须维护其知识产权；私密信息的价值在于可靠，必须维护其安全。互联网的发展极大促进了信息的生产和传播，但往往难以证明共享信息的真伪，难以确认专有信息的所有权，难以保护私密信息的安全。

区块链的分布式功能，通过构建分布式数据库系统和参与者共识协议，有利于保护数据的完整性。区块链的时间戳功能，通过生成一定时间段的信息区块和区块之间首尾相连的数据链，能够形成可追本溯源、可逐笔验证、不可篡改、不可伪造的数据；每个参与者在生成信息区块时加盖时间戳，能够证明原创性和所有权归属。区块链的非对称加密功能，有利于保护信息的私密性。

龚鸣编著的《区块链社会：解码区块链全球应用投资案例》一书，

为人们描述了区块链技术实际应用的场景和案例。可以让更多的人了解区块链，了解区块链将会如何改变我们的生活。

例如，Circle China、Abra将区块链技术应用用于跨境支付汇款这个生活中经常出现的场景，节省了跨境汇款的时间成本、人力成本，使跨境汇款更加便捷。Symbiont通过智能合约自动生成智能证券，在区块链之上自动完成证券的发行、交易和结算，让证券交易变得简单直接，能够更有效的保护合约，防止信息泄露。在奢侈品溯源、分布式交易所、物联网和供应链、医疗行业、互助保险等领域，区块链技术应用都有可能成为现实。

国务院《推进普惠金融发展规划（2016-2020）》提出：“金融基础设施是提高金融机构运行效率和服务质量的重要支柱和平台，有助于改善普惠金融发展环境，促进金融资源均衡分布，引导各类金融服务主体开展普惠金融服务。”应用区块链技术，可能形成新的技术优势：成本较低，风险较小；数据完整，信息透明；智能化管理和监控。这将提升金融基础设施的服务功能，有利于推进普惠金融发展。

万向区块链实验室计划出版一系列区块链丛书，推广这一项在中国还有些陌生，但未来也许会改变世界的区块链技术。我们感谢万向区块链实验室所做的贡献。

[\[1\]](#)李礼辉，全国人大财经委员会委员，中国银行前行长，中国互联网金融协会区块链研究工作组组长，有近40年金融工作经验。

序二 区块链的研究与应用并重

王永利^[1]

一段时间以来，常常在微信圈里看到龚鸣兄（暴走恭亲王）发布的关于全球范围内区块链在多个领域应用的案例，深受启发，也特别佩服他花费那么多时间和精力收集和整理了那么多区块链应用的案例，更希望他能将这些成果进一步整理提炼，形成系统的成果并更广泛地传播。近期获知，在此基础上，他即将出版发行《区块链社会：解码区块链全球应用与投资案例》，深感欣喜，相信此书的发行，一定会为人们了解和认知区块链，特别是区块链可能的应用和投融资领域，提供很大帮助，发挥重要作用。

现在，区块链已经成为互联网领域，特别是金融科技（Fintech）领域火热的概念，吸引了越来越广泛的关注、研究乃至投资热潮。但客观讲，区块链技术自2009初随比特币首次推出并付诸应用开始，现在应用的时间还很短，而且比特币完全是模拟黄金，在独立的网络世界重构出一种数字货币或数字资产（财富），比特币一开始并不是可以直接用法定货币购买到的，而必须先比特币社区（Block）通过“挖矿”的方式产生；挖到的比特币，必须用比特币合约规定的相互认证方式加以确认（去中心化），包括所有者的身份认证与其比特币数量的认证等，而不是用现实世界惯用的主权国家公民身份证等证件，由业务或鉴证中心予以确认；比特币的转让交易，采用全网加密、分布式记账方式加以确认和记录，其中包括跨区块之间的交易，必须加入区块的加密代码以及时间代码等，形成区块之间的连接（即Blockchain，区块链）；在形成独特的比特币世界（包括参与者的身份认证、比特币的产生和交易认证和记录、相关的管理规定等形成的体系）之后，才开始推动比特币世界与

现实世界的连接，允许比特币与法定货币的兑换与交易。可见，区块链在比特币上的应用，是不受现实世界各种规制约束的，是在人为创造的独特环境中的应用。因此，尽管区块链在比特币上得到了可以说非常成功的应用，但是，要将其直接应用到现实世界，却可能受到非常多和大的约束，甚至不可避免地会面临诸多挑战和阻力，是会非常艰难的。对此，必须要有清醒的认识，不能盲目追崇和胡乱投资。

但是，区块链和比特币的出现，确实给人们认识和适应新兴的网络世界带来思维方式和路径上的巨大冲击或创新：由于网络世界是在现实世界基础上随着互联网的发展而出现的，各种财富和交易，都是从线下向线上迁移和推广的，因此，线上的当事人身份认证、交易确认、资金清算和交易记录等等，也就非常自然的沿用线下的规则，或进行必要的改造以适应网络运行的需要。但随着网络世界的发展和交易的日益频繁，人们逐步发现，完全沿用线下规则，很难适应和满足线上的需求，亟需有更大的革新乃至革命，创造出不同于现实世界的全新的网络世界。在这方面，区块链和比特币的出现，即使还存在这样或那样的问题，其全新的思维和实践方式，却具有极其重大的启蒙意义。因此，非常有必要不断加强和加深对区块链的研究和创新，特别是寻求如何将现实世界的财富向网络世界迁移并扩大交易的可行的高效的路径与方式。

《区块链社会：解码区块链全球应用与投资案例》一书，不仅对区块链的概念和原理进行了必要的梳理，更重要的是提供了大量具有典型意义的全球应用与投资案例，突出研究和应用并重，并作为重要的研究结论，提出区块链可能成为人类首次大规模协作和相互认证的开始，分布式记账方式、去中心化自治组合和智能合约，也许会颠覆现代商业社会，重塑社会结构和运行方式。相信，这会给读者带来很多启发。

祝愿《区块链社会：解码区块链全球应用与投资案例》发行成功，也期待龚鸣兄更多的研究成果面世！

[1] 乐视高级副总裁，中国银行股份有限公司前执行董事、董事会风险改革委员会委员及副

行长。

序三 区块链：数字另类资产的新大陆

肖风^[1]

你一定知道美国著名高校耶鲁大学。如果你对她稍作了解，你一定也听说过耶鲁大学基金会。如果你对基金投资稍作了解，你一定看到过耶鲁大学基金会过去几十年骄人的投资业绩。作为大学捐赠基金，因为资金的长期性，它的投资目标第一是要打败通胀，第二是要战胜基准，第三是要力争绝对收益。可喜的是，这三条耶鲁大学基金会都做到了！尤其第一、第二条目标，更是大大超越！

研究早已表明，超过90%的投资业绩的取得，来自于资产配置，而不是来自于个股或个券的选择。耶鲁大学基金会几十年的骄人投资业绩，就来自于他们在资产配置模式上的大胆创新。据耶鲁大学基金会2015年年报披露，该基金截止2015年6月的资产组合中，大宗商品占比6.7%；私募股权占比32.5%；房地产占比14%；合计超过组合的50%。在全球资产管理界的经典教科书上，我们一般把股票、债券、现金归为传统资产类别，而把大宗商品、对冲基金、PEVC、房地产归于另类资产类别。人们把这种以另类资产作为组合核心资产来配置的新模式，叫做“耶鲁模式”，以区别于以股票、债券、现金等传统资产为组合核心资产来进行配置的资产配置模式。耶鲁大学基金会超越同行、超越基准目标的大部分秘密就在这里！

从耶鲁大学基金会的案例里，我们可以得到三点启示：一、要得到比别人更高的投资回报，就不能只在传统资产类别里打转，要另辟蹊径；二、资产类别不是一成不变的，新技术、新经济、新模式会创造出新的资产类别，要有独到眼光；三、如何对新的资产类别进行评估分

析，进行风险定价，要有新的框架、新的方法。谁比别人更快更好的掌握了新方法，谁就可以饮到头啖汤！

我们知道，十五、十六世纪的地理大发现，奠定了欧洲大陆近几百年在人类社会的领先地位，为欧洲大陆创造了至今仍然可观的物质财富。而自从互联网技术于上个世纪九十年代初成熟以来，人类社会又开始了一次新的地理大发现运动。这次不再是物理空间的大发现，而是数字空间的大发现。上世纪九十年代中，MIT媒体实验室负责人尼葛洛庞帝出版的《数字化生存》，是这场数字地理大发现的行动宣言。传统的依靠土地、设备、劳动力创造财富的模式，因为资源的有限性，已经无以为继。而数字空间的无限可扩展性、比特结构的无限可复制性、虚拟世界的多维可塑性可能意味着蕴藏在这里面的待开发的财富，会数十倍于物理世界！

这些新财富的表现形式就是数字资产！

什么是数字资产？我认为数字资产有五个属性：第一，数字资产是登记在区块链账本或分布式账本上的资产，那些登记在工商局的股权，登记在房产局的房产一定不是数字资产；第二，数字资产是以比特结构存在的虚拟资产，不是像黄金那样具有原子结构的实物资产；第三，数字资产是一段计算机程序，不再是一行数字符号，可以对它进行编程，资产之间的交换是代码与代码的交换，不是数字之间的增减；第四，数字资产因为可编程性，可以在区块链上，通过编制智能合约程序，完全去中介化的自主、自治的进行点对点交易，不需要人工干预；第五，数字资产大部分情况下都是以“Coin”（数字代币）的形式存在的，数字资产跨越了资产证券化的阶段，直接达到了资产货币化的阶段。

比特币、以太币等数字货币是目前最为人们熟悉的一类数字资产。各式各样的数字货币大概有三百多种，市值约一百二十亿美元。但数字资产的范围比这要大得多。欧美主流金融机构几乎都成立了自己的区块链实验室，正在各种金融场景中，试验运用区块链技术，来创设发行智

能股票、智能债券。所谓智能，其实就是利用区块链的数据不可更改性和可编程性，在区块链上登记发行股票或债券，使得这些数字化了的股票或债券，可以依靠智能合约点对点自主交易，自我结算。在另一条跑道上，还有许多推崇完全去中心化，希望在数字世界里建立一个完全自由、自主、自治的体系的技术极客们，也在尝试推出形形色色的数字资产。根据IBM于2014年发布的物联网白皮书《设备民主》预测，到2050年将会有1000亿台设备连网在线，届时在区块链的管理下，将可以实现设备对设备的金融交易（M2M），这更是一个创设、发行、交易数字资产的更大的机会。

在这里，我可以做一个乐观的展望：十年之后，数字资产整体的市值预计可以达到一万亿美元！到那时，数字资产必将成为另类资产其中的一个举足轻重的类别。谁忽略数字资产，谁不把数字资产列入自己的资产组合，那谁的业绩回报就难以超越基准、超越同行。我们也许可以大胆的预言：从资产组合回报的角度来看，未来十年，如果你的组合资产配置当中没有纳入数字资产，也许你就真的输在起跑线上了！

我想，我们一定可以在未来十年当中的某一年，在耶鲁大学基金会的年报上，看到数字资产作为另类资产的新类别，加入到了基金的资产组合中。

龚鸣（网民“暴走恭亲王”）先生是中国最早一批数字货币和区块链技术的研究者和实践者之一。近年来，他致力于在中国推广、传播、培训区块链的理论知识、行业资讯和创业信息，无远弗届。为中国区块链行业的发展做出了突出贡献！并且他自己身体力行，创办了中国第一家专注于区块链技术的媒体——区块链铅笔，成为了中国区块链行业的创业者之一，胆识可佩！勇气可嘉！

欣闻他撰写的著作《区块链社会：解码区块链全球应用与投资案例》即将由中信出版社出版，着实令人高兴！借为这本书写推荐序的机会，有幸提前拜读了书稿。这也许是全球第一本全景式介绍区块链行业

情况，尤其是创业公司情况的书籍；这也许是全球第一本全景式介绍区块链行业投资情况的书籍。龚鸣先生毫无保留地把他过去几年对全球区块链行业的观察和研究心得，几乎是和盘托出。因此，这本书可以帮助我们认清数字资产的性质内容、看清数字资产的形成过程、把握数字资产的投资机会、形成数字资产的投资方法。

在此，作为一个区块链技术的中国信徒，我要感谢他的付出！

在此，郑重的向大家推荐这本书！

[\[1\]](#)肖风，南开大学经济学博士，中国万向控股有限公司副董事长，万向区块链实验室和分布式资本的创始人。

前言

自从去年参与翻译了《区块链——新经济蓝图》之后，到现在为止，“区块链”这三个字已经从极小的极客圈中走出，开始变成一个越来越火热的概念。无论是国内还是国外，都掀起了对区块链技术普及和探索的新高潮，越来越多的人开始注意到这个新技术可能产生的巨大影响。但也有更多的人，表现出了极大的困惑，因为往往在看介绍区块链相关文章的时候，觉得这个技术似乎可以彻底颠覆世界，但是如果真的在现实世界中试图探寻可落地的应用案例，却又似乎很难找到身边有价值的案例。我在许多场合中发现，很多试图了解区块链行业的人最容易产生的疑惑就是，区块链，究竟是真的会成为改变许多商业模式的神奇工具，还是仅仅是又一个包装出来的全新概念。

而本书，就试图针对这个疑惑给出一个我的答案。相对而言，国外在区块链技术上，已经完全走出了普及阶段，而早已是真金白银的大量投入。不仅仅可以看到许多大型金融机构和央行投入巨大的人力和物力到其中，而且许多有趣的创业公司开始兴起。除了比特币和以太坊之外，区块链已经在非常多的领域大规模开始尝试，在本书中你可以看到非常多有趣的项目案例。除了经常能够看到的金融行业案例之外，还包括物联网、公证、医疗、保险、能源等非常多的领域。并且其中的许多尝试，恐怕会彻底颠覆一些传统商业模式的思维。无论是能够提供按分钟跨国工资发放方案来彻底杜绝拖欠工资可能性的BitWage，建设完全去中心化的自治电子商务市场OpenBazaar，或者是提供锚定SDR来实现稳定数字货币的Maker项目，以及登记全球钻石信息防止血钻交易的Everledger项目，都让人有耳目一新的感觉。如果有时间深入研究这其中许多案例的话，最终都可以得出同样的结果，即区块链的本质是一个大规模协作工具，绝不仅仅是改变一两个行业，而是最终会改变我们全

球所有人的协作模式。

但是也有许多朋友经常问我，究竟目前有哪些领域有落地的区块链项目开始大规模应用和部署？非常遗憾，现在可能还没有任何区块链项目开始广泛应用或部署。事实上，就像互联网初期，在95、96年的时候，互联网似乎除了看新闻之外并没有太大的作用。特别是互联网开始发展阶段出现大量烧钱的行为，尽管不断有新的模式出现，但始终无法盈利，让很多人最终开始怀疑互联网究竟是不是就是噱头而已，并且导致了互联网第一次泡沫的破裂。而到了今天，应该没有任何人再会怀疑互联网是不是只能用来看看新闻。同样，区块链也在经历一样的过程，尽管我们的直觉告诉我们，这似乎是一个具有极大潜力的工具，但是现在除了比特币之外，我们并没有看到非常广泛的落地应用出现。事实上，区块链作为一个行业崛起，在初期还有大量的基础工作要做。就如同在95、96年，如果你期盼马上看到淘宝、京东未免还太早，更不用说微信这样的应用了。这都需要整个生态环境逐渐建立起来，才能够开始出现一些能够改变我们生活的应用。而又要经过相当一段的普及时间，才能够让更多人开始意识到生活逐渐被技术所改变。不过，需要注意的是，技术始终是以加速度而不是匀速来发展的，也许不需要再等五六年才能看到第一次高潮的来临，也许对于区块链行业而言，再有2、3年的时间就可以完成第一次的技术积累。

本书在介绍区块链世界中的众多案例时，希望大家能够注意到这个行业中始终有两条路线的斗争在进行中。第一条是自上而下的路线，我们所能看到的类似于R3 CEV，HyperLedger这样的联盟，这都是大型金融机构为了确保自己在这场未来变革中的既得利益者位置，而所作出的努力。在今天的世界上，金融行业内聚集了全世界最聪明的一群人。不同于互联网初期，全球邮政机构不愿意接受电子邮件，从而最终成为互联网变革中第一个倒下的恐龙。而今天的金融行业，已经从区块链技术的发展中嗅到了一丝危险的味道，他们并不像传统邮政系统拒绝变化，而是愿意拥抱变化，甚至是主导变化。但是他们的要求就是，在未来的

世界中，依旧获得足够的主导权，并且由他们来决定技术的发展方向。

另外一条路线是一条自下而上的路线，从比特币开始，到Ethereum、BitShares都显然是其中的代表。由于区块链技术本身是来自比特币，似乎始终能从区块链技术中感受到一股桀骜不驯的力量。这条自下而上的路线中的许多项目，完全无视现有的商业规则和既定的商业模式，用一种完全不同于过去思路在进行快速发展，并且颠覆了许多人对很多传统商业模式原有的思考方式。更进一步的是，这条路线甚至彻底颠覆了融资方式，不同于云计算、大数据，甚至是今天火热的VR、AR这样的技术变革，因为他们最终会需要通过VC、PE的传统方式来进行融资。而作为一种极具生命力的方式，区块链自下而上路线中的许多项目选择了ICO（Initial Coin Offering）的方式来进行融资，从而形成了一个完整且自给自足的资金循环体系。而这也是让许多传统金融机构和监管机构深感不安的地方，而本书也有专门的章节会对ICO方式进行详细的介绍。

此外，许多区块链项目是如何盈利的也经常困扰刚刚开始了解这个行业的人们，由于许多ICO的区块链项目通常使用燃料货币来运作，因此已经完全没有了盈利、利润这样的概念，甚至不再有公司的概念。这让许多人一时间完全无法转换自己的思维定式。本书也会针对燃料货币理论，首次进行深入的剖析和讲解。

纵观整个IT技术的发展，技术路线的选择往往有许多的偶然性，所以现在我们也难说是哪条路线会赢得最终的胜利，亦或是两种技术最后会互相妥协和互相融合。但是，正是由于每条路线都感到了对方所带来的巨大压力，从而自身也催生出巨大的发展动力。我们相信无论最终结果如何，这个世界中将都会被区块链所彻底改变。

许多人问我如何看待比特币未来的发展，以及比特币和区块链之间的关系。比特币目前是整个区块链行业中最重要的一部分，其市值占有区块链世界中所有数字资产近百分之九十的份额。但很明显，随着区块链

技术的发展和层出不穷的区块链项目，比特币这样的中心化地位肯定会被进一步削弱。但这不代表比特币本身不再发展，比特币依旧会继续完善它自己的生态环境，并且会变得越来越实用，有更多的人会开始使用比特币，相关的应用也会越来越多。只不过，其它不同的区块链项目相对比特币而言发展的更快，并且会扩展到越来越多的领域中，区块链世界中比特币一家独大的局面很可能会一去不复返。

在国内早期介绍和宣传区块链时，往往也会面临许多的不理解，甚至被很多国内的人指责为骗局。在2013年前后，我还专门成立过以志愿者为主的翻译小组，翻译来自互联网上与数字货币和区块链相关的各类资讯。其中有许多人在开始翻译时，对行业充满热情。但是，尽管是在为大家免费翻译资料，还是会经常饱受各种指责和攻击，因此许多人也陆续离开了翻译团队。本书在写作时也参考了互联网上的一些相关资料，其中有些资料并不能一一确定出处，据我所知，也有部分资料的翻译者已经离开了这个社区，我也借本文再次感谢这些曾经在互联网上为大家免费翻译的贡献者。我本人在宣传区块链的几年里，也不时受到一些苛责，但有幸从未放弃过让更多人了解区块链的目标，并且现在还运营名为“区块链铅笔”的区块链行业门户网站和微信公众号，让更多的人可以有机会来了解行业的最新动态。

最后，我非常感谢这本书在写作时，许多人给予我的帮助，特别是万向区块链实验室和分布式资本的许多领导和朋友给予我的指导和支持，互联网金融协会区块链小组的领导们对本书的支持，我们区块链铅笔的同仁们也参与了本书的校对，也非常感谢我的家人在我写作时对我的支持。最为感谢的还是许多关心区块链的朋友们一直努力在微信群里对我的支持和鼓励，是大家的支持始终让我有不断写作的动力。

龚鸣

第一章 区块链：信任的机器

一、为什么会出现区块链

区块链是比特币的一个重要概念，其初始使命是为了支持比特币的形成和流通。在比特币诞生之前，互联网的TCP/IP（传输控制协议/因特网互联协议）协议，基本实现了全球信息传递高速低成本的传输，而有一类特殊的信息——货币则无法在上面进行高速传输。本质原因在于，传统互联网是信息互联网，而不是价值互联网。

互联网诞生之初，最先解决的核心问题是信息制造和传输。1992年，时任美国副总统阿尔·戈尔（Albert Amold Gore Jr.）提出美国信息高速公路的想法。1993年9月，美国政府宣布实施一项新的高科技计划——国家信息基础设施（National Information Infrastructure, NII），旨在以当时简单互联网为雏形，建设信息时代的高速公路——信息高速公路，使所有的美国人可以方便地共享海量的信息资源。

随着该项计划的发展，我们现在所熟悉的网络世界逐渐形成。在这个“高速公路”上，我们能够将信息快速生成并且复制到全世界每一个角落，这也是我们现在的互联网网络最擅长的事情，所以也可以将其称为“信息互联网”。在这个“信息互联网”上，所有传递的信息都是可以高效传播和复制的，从而构成互联网的基础协议——TCP/IP。在容许一定错误率的情况下，以最快的速度把信息传递或者复制到目标地址。而当时我们正处于一个非常“渴求”信息的时代，只要能将信息快速传播和复制就实现了我们最基本的需求。从此，我们通过“信息互联网”进入到一个“信息爆炸”的时代。整个互联网上的信息开始以几何式

的速度增长，信息的复制和分享成为这个时代的主流。

然而，随着互联网开始进入人类生活的各个层面，我们发现有些信息是无法复制的，或者说复制是没有意义的。比如货币支付，我们不能把要支付的钱直接复制到对方账户上，而是一定要在付款账户上减去若干资金，然后在收款账户上增加若干资金。只有这样，这个支付行为才是有意义的，而不像新闻类信息，我们复制一份到新的网站上，就有了两份信息，可以让更多的人来进行分享。而这些不能分享，只能转移的信息，往往具有更大的价值，在它的背后需要有信用作背书，从而产生价值。因此，可以发现，我们的“信息互联网”非常善于处理“信息分享”，而不能解决“价值转移”或者说“信用”这件事情。

这里所谓的“价值转移”是指，在网络中以每个人都能够认可和确认的方式，将某一部分价值精确地从某一个地址转移到另一个地址，而且必须确保当价值转移后，原来的地址减少了被转移的部分，而新的地址增加了所转移的价值。这个“价值”可以是货币资产，也可以是某种实体资产或者虚拟资产（包括有价证券、金融衍生品等）。而这种操作的结果必须获得所有参与方的认可，且其结果不能受到任何某一方的操纵。

从以上的定义可以发现，目前互联网本身的协议并不支持这个“价值转移”功能。互联网TCP/IP协议无法确认当信息发出去后本地的数据是否会精确改变，而某单点的数据篡改在现有的互联网系统中是很难被全网发现的。但是“价值转移”是金融系统的基础，而金融系统是人类生活的核心之一，因此下一代全球性互联网发展的核心问题就是要解决“价值转移”的问题。

二、“价值转移”的本质

在没有解决这个问题之前，我们必须使用中介系统来完成这样的“价值转移”行为，于是我们看到了类似于支付宝、贝宝（Paypal）的第三方支付工具开始崛起。而在跨国汇款领域，大家更多的是通过类似于SWIFT（环球同业银行金融电讯协会）这样的中介机构来完成跨国汇款结算和清算。

互联网中也有各种各样的金融体系，也有许多政府银行或者第三方提供的支付系统，但是它还是依靠中心化的方案来解决。所谓中心化的方案，就是通过某个公司或者政府信用作为背书，将所有的价值转移计算放在一个中心服务器（集群）中，尽管所有的计算也是由程序自动完成的，但是却必须信任这个中心化的人或者机构。事实上，通过中心化的信用背书来解决，也只能将信用局限在一定的机构、地区或者国家的范围之内。由此可以看出，要解决这个根本问题，就必须建立“信用”。所以价值转移的核心问题其实就是跨国信用共识问题。

但根据历史经验来看，整个系统中往往最不可信任的就是人，或者由人组成的机构或政府，历史往往最终被证明，那些违反原规则的人就是规则制定者，而从工业革命到互联网革命，技术发展的潮流也是通过取代人这个最不可靠、最脆弱且效率最低的环节来实现生产力大发展的。所以，归根结底，要真正完成以信用共识为基础的价值转移，需要一个能够取代第三方中介的方式，一个能够自动运行的方式，且具备去信任的机制（不需要依靠相信环节中的任何人或机构）的机制来完成价值的转移。

在如此纷繁复杂的全球体系中，要凭空建立一个全球性的信用共识体系是很困难的，由于每个国家的政治、经济和文化情况不同，两个国

家的企业和政府建立完全互信几乎是不可能做到的，这也就意味着无论是以个人或以企业、政府的信用进行背书，对于跨国的价值交换即使可以完成，但也需要很长的时间和高昂的经济成本。但是在漫长的人类历史中，无论每个国家的宗教、政治和文化如何不同，唯一能取得共识的是数学（基础科学）。因此，可以毫不夸张地说，数学（算法）是全球文明的最大公约数，也是全球人类获得最多共识的基础。如果以数学算法（程序）作为背书，让所有的规则都建立在一个公开透明的数学算法（程序）之上，那么就能够让所有不同政治文化背景的人群获得共识。

三、什么是区块链

（一）定义

区块链本质上是一个去中心化的数据库，是一连串使用密码学方法产生相关联的数据块，每一个数据块中包含了一段时间内全网交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。所以说区块链是以去中心化和去信任化的方式，来集体维护一个可靠数据库的技术方案。

通俗地说，其实区块链可以称为一种全民记账的技术，或者说可以理解作为一种分布式总账技术。

数据库是大家都熟悉的概念，任何的网站或者系统背后都有一个数据库，我们可以把数据库想象为一个账本，例如支付宝数据库就像是一个巨大的账本，里面记录每个人账上有多少钱。当A发送给B一元钱，那么就要把A账上的钱扣除一元，在B的账上增加一元，这个数据的变动就可以理解为一种记账行为。对一般中心化的结构来说，微信背后的数据库由腾讯的团队来维护，淘宝背后的数据库由阿里的团队来维护，这是很典型的中心化数据库管理方式，也是大家认为顺理成章的事情。

但是区块链完全颠覆了这种方式。一个区块链系统由许多节点构成，这些节点一般就是一台计算机。在该系统中，每个参与的节点都有机会去竞争记账，即更新数据库信息。系统会在一段时间内（可能是十分钟，也可能是一秒钟），选出其中记账最快最好的一个节点，让它在这段时间里记账。它会把这段时间内数据的变化记录在一个数据区块（block）中，我们可以把这个数据区块想象成一页纸。在记完账以

后，该节点就会把这一页的账本发给其他节点。其他节点会核实这一页账本是否无误，如果没有问题就会放入自己的账本中。

在系统里面，这一页账本的数据表现形式，称为区块，该区块中就记录了整个账本数据在这段时间里的改变。然后把这个更新结果发给系统里的每一个节点。于是，整个系统的每个节点都有着完全一样的账本。

我们把这种记账方式称为区块链技术或者分布式总账技术。

（二）安全性

那么，为什么要采取这种方式？它有什么优势？因为通常大家的直觉是，这种方式似乎会较为浪费带宽和存储空间，并不是一个可取的方案。但是，区块链就是通过这种高冗余的方式来构建极高的安全性。

首先，每个节点的权利是一样的，任意节点被摧毁都不会影响整个系统的安全，也不会造成数据的丢失。每个节点在系统中的权重都是一致的，系统每次都在链入这个系统的节点中选择记账者，于是，即使某个或者部分节点被摧毁、宕机都不会影响整个系统运作。

其次，每个节点的账本数据都是一模一样的，也就意味着单个节点的数据篡改是没有任何意义的。因为如果系统发现两个账本对不上，它就认为拥有相同账本数量较多节点的版本才是真实的账本数据。那些少部分不一致的节点账本不是真实的，而是被篡改的数据账本。系统会自动舍弃这部分认为被篡改过的账本，也就意味着如果你要篡改区块链上的数据内容，除非能够控制整个系统中的大部分节点。这也就是常说的51%攻击，即必须要控制整个系统50%以上的节点，才能发动对数据账本的篡改。

但是，当整个系统中的节点数量高达成千上万个，甚至是数十万个时，那么篡改数据的可能性就会大大降低。因为，这些节点很可能分布在世界上每个角落，理论上说，除非你能控制世界上大多数电脑，否则你没有机会去篡改区块链上的数据。

此外，另一个51%攻击的方法就是构建出和原来系统一样多节点（算力）的方式来攻击这个区块链系统（尽管重要的是要构建足够大的算力，而不仅仅是节点数量，但考虑到算力概念理解更加复杂，这里就以节点数量来做比喻）。比如，该系统原来有10000个节点，那攻击者部署另外10001个节点，然后加入到这个区块链系统中。由于攻击者已经获得了超过50%的控制权，就能够发动攻击。显然，这种攻击所付出的成本也取决于系统原来的大小。原来系统节点越多，攻击者付出的成本也越大。由于比特币是目前最庞大的区块链网络，据统计要构建出一个和现有比特币同样大型的网络系统，所付出的成本会高达270亿美元。

但是攻击者还面临着另一个困境，一旦它成功发动攻击后，就会造成该系统的价值瞬间归零。也就是说，一旦攻击者成功篡改账本，由于全网能够立刻识别出账本数据不一致，导致所有人都意识到该系统账本已经是不可靠的账本，那么就意味着该账本所记录的数据变得没有价值，该系统中的代币也会变得毫无价值。也就是说，如果攻击者付出了超过270亿美元的代价，成功发动了对比特币的攻击后，比特币价格瞬间归零，那么攻击者也无利可图。而对于国家而言，似乎也没有必要通过这种方式来攻击比特币这样的网络，国家完全可以通过直接宣布比特币违法来更简单地达到禁止比特币这一目的。

（三）起源

大多数人都知道区块链和比特币关系密切，甚至有些人会把区块链

等同于比特币技术。事实上，区块链技术仅仅是比特币的底层技术，是在比特币运行很久之后，才把它从比特币中抽象地提炼出来。从某种角度来看，也可以把比特币认为是区块链最早的应用。

比特币的创造者——中本聪（Satoshi Nakamoto）在其2008年发表的经典论文《比特币：一种点对点网络中的电子现金》中明确指出：传统的金融体系不可避免地要依赖“第三方”机构（传统银行），这种传统的中心化金融结构是很难让货币像其他信息那样免费地进行传输。正是为了解决这些问题，中本聪创造性地提出了通过区块链技术建立一个去中心化、去第三方、集体协作的网络体系设想，而无须中心化平台做信任的桥梁，区块链通过全网的参与者作为交易的监督者，交易双方可以在无须建立信任关系的前提下完成交易，实现价值的转移。如果说互联网TCP/IP协议是信息的高速公路，那么区块链的诞生意味着货币的高速公路第一次建设已经初步形成。

就像核工程的研究最初是为了制造原子弹，而后人们才意识到其更大的社会价值是对于全球能源体系的改造。近年来，全球开发者、金融机构、企业乃至政府发现区块链的意义不仅局限于支持比特币交易，通过区块链技术所打造的成本极低的、去中心化、去第三方、集体协作的网络体系本身还具有巨大的社会价值。

《经济学人》把区块链技术形象地比喻为“信任的机器”，即可以在没有中央权威的情况下，对彼此的协作创造信任。区块链技术适用于一切缺乏信任的领域，也许在未来会成为全球人类文明信任的基石，并有可能彻底改变全球的社会结构。目前，随着区块链技术的成熟和演进，区块链的应用场景不再局限于比特币，以“以太坊”为代表的新一代区块链技术正在开始构建一个全新的去中心化互联网架构，试图彻底颠覆所有的互联网中心化架构平台（如支付宝、银行、保险等）。

四、比特币的底层技术

在过去的一年中，尽管比特币本身受到质疑，然而人们开始从比特币的支付领域逐渐转移到了比特币底层协议——区块链技术上，越来越多的投资者及普通民众接受了区块链的概念。我们可以通过了解比特币的生成与交易等一系列过程来理解区块链技术。

（一）比特币的交易

比特币使用整个P2P（互联网金融点对点借贷平台）网络中众多节点构成的分布式数据库，来确认并记录所有的交易行为。在信息传递过程中，发送方通过一把密钥将信息加密，接收方在收到信息后，再通过配对的另一把密钥对信息进行解密，这就保证了信息传递过程的私密性与安全性。比特币的交易并非简单的支付货币本身。以图1.1中的交易为例，如果B想支付100个比特币给C，那么不仅B需要在交易单上注明金额，而且需要注明这100个比特币的来源。由于每笔交易单都记录了该笔资金的前一个拥有者、当前拥有者以及后一个拥有者，就可以依据交易单来实现对资金的全程追溯。这也是比特币的典型特征之一。最后，当每一笔交易完成时，系统都会向全网进行广播，告诉所有用户这笔交易的实施。

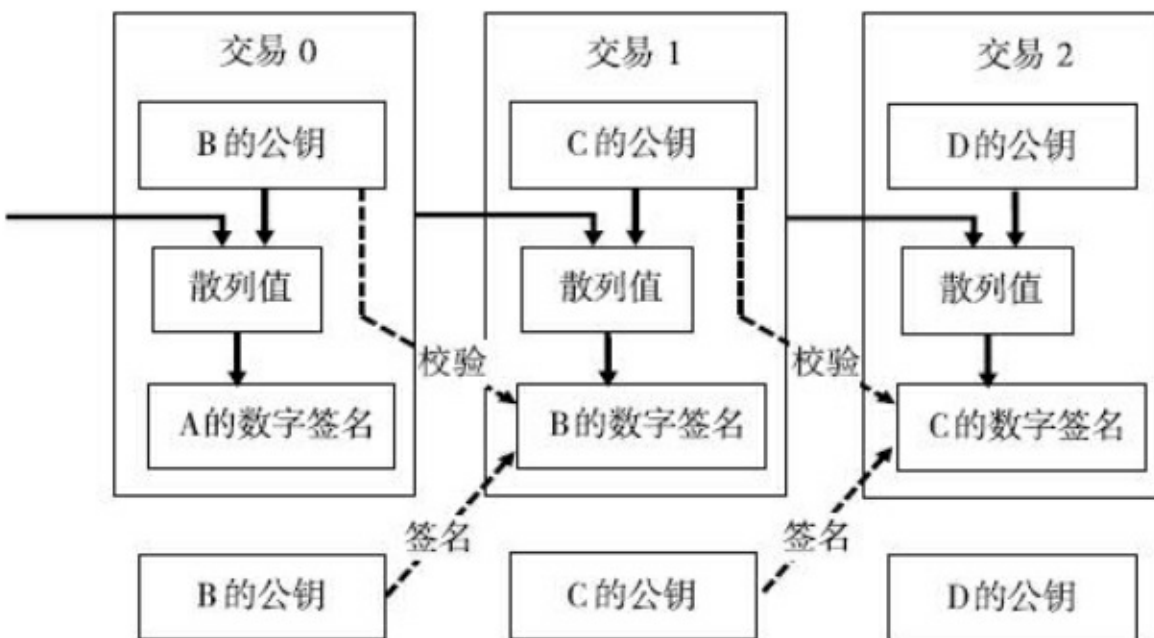


图1.1 比特币的交易过程

（二）区块+链

由于每笔交易是相对分散的，为了更好地统计交易，比特币系统创造了区块这一概念。每个区块均包含以下三种要素：一是本区块的ID（散列），二是若干交易单，三是前一个区块的ID。比特币系统大约每10分钟创建一个区块，其中包含了这段时间里全网范围内发生的所有交易。每个区块中也包含了前一个区块的ID，这种设计使得每个区块都能找到其前一个节点，如此可一直倒推至起始节点，从而形成了一条完整的交易链条。因此，从比特币的诞生之日起，全网就形成了一条唯一的主区块链，其中记录了从比特币诞生以来的所有交易记录，并以每10分钟新增一个节点的速度无限扩展。这条主区块链在每添加一个节点后，都会向全网广播，从而使得每台参与比特币交易的电脑上都有一份拷贝。在现实世界中，每笔非现金交易都由银行系统进行记录，一旦银

行计算机网络崩溃，所有数据都会遗失。而在互联网世界中，比特币的所有交易记录都保存在全球无数台计算机中，只要全球有一台装有比特币程序的计算机还能工作，这条主区块链就可以被完整地读取。如此高度冗余的交易信息存储，使得比特币主区块链完全遗失的可能性变得微乎其微。

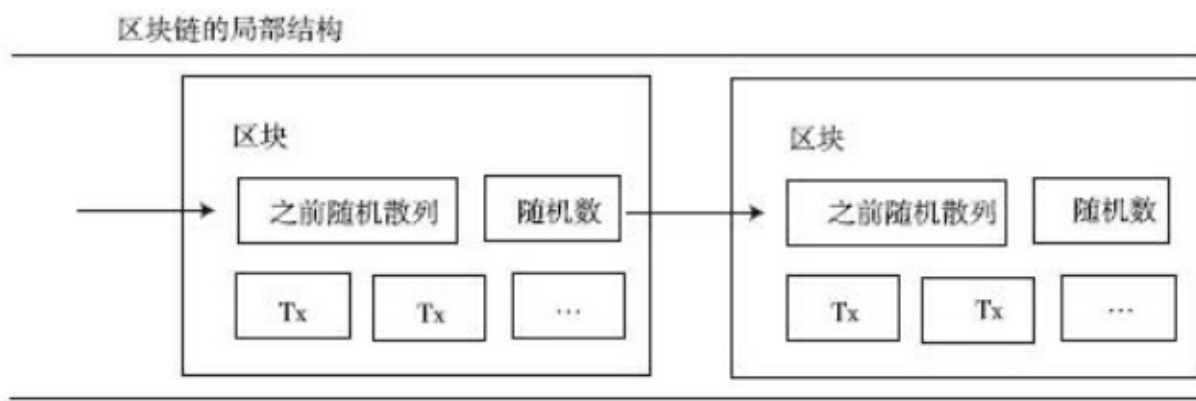


图1.2 区块链的局部结构

资料来源：Bitcoin: A Peet-to-Peer Electronic Cash System

每个人在对交易的有效性进行验证后都可以根据这些交易数据生成新区块。为了避免虚假交易或重复交易，使这一新区块被信任，需要构建工作量证明机制。如果想要修改某个区块内的交易信息，就必须完成该区块及其后续连接区块的所有工作量，这种机制大幅提高了篡改信息的难度。同时，工作量证明也解决了全网共识问题，全网认可最长的链，因为最长的链包含了最大的工作量。

（三）比特币与区块链

综上所述，区块链是一串使用密码学方法相关联产生的数据块。在比特币的应用中，整个区块链就是比特币的公共账本，网络中的每一个节点都有比特币交易信息的备份。当发起一个比特币交易时，信息被广播到网络中，通过算力的比拼而获得合法记账权的矿工将交易信息记录成一个新的区块连接到区块链中，一旦被记录，信息就不能被随意篡改。比特币是区块链的一个“杀手级应用”，区块链是比特币的底层技术，且作用绝不仅仅局限在比特币上。因此，尽管比特币与区块链经常被同时提及，但二者并不能画上等号。

五、区块链的模型架构

区块链系统由自下而上的数据层、网络层、共识层、激励层、合约层和应用层组成（如图1.3所示）。

（一）数据层

数据层封装了底层数据区块的链式结构，以及相关的非对称公私钥数据加密技术和时间戳等技术，这是整个区块链技术中最底层的数据机构，其中大多数技术都已被发明数十年，并在计算机领域使用了很久，无须担心其中的安全性，因为如果这些技术出现安全性上的巨大漏洞，则意味着全球金融技术都会出现严重的问题。中本聪在设计比特币时，为每个区块设置了1MB（兆）大小的容量限制，但由于目前比特币的交易量迅速提升，1MB的区块空间能容纳的交易数量有限，所以要考虑扩容区块链来突破这个限制。



图1.3 区块链系统数据层

（二）网络层

网络层包括分布式组网机制、数据传播机制和数据验证机制等，由于采用了完全P2P的组网技术，也就意味着区块链是具有自动组网功能的。这种P2P组网技术，在早先应用于BT（比特流）和eMule（电驴）之类的P2P下载软件中，也是一种相对来说非常成熟的技术。

（三）共识层

共识层主要封装网络节点的各类共识机制算法。共识机制算法是区块链技术的核心技术，因为这决定了到底由谁来进行记账，记账者选择方式将会影响到整个系统的安全性和可靠性。目前已经出现了十余种共识机制算法，其中最为知名的有工作量证明机制（Proof of Work, PoW）、权益证明机制（Proof of Stake, PoS）、股份授权证明机制（Delegated Proof of Stake, DPoS）等。在下一节中将会详细介绍这些共识机制。

（四）激励层

激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等，该层主要出现在公有链（Public Blockchain）中，因为在公有链中必须激励遵守规则参与记账的节点，并且惩罚不遵守规则的节点，才能让整个系统朝着良性循环的方向发展。所以激励机制往往也是一种博弈机制，让更多遵守规则的节点愿意进行记账。而在私有链（Private Blockchain）中，则不一定需要进行激励，因为参与记账的节点往往是在链外完成了博弈，也就是可能有强制力或者有其他需求来要求参与记账。

（五）合约层

合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础。以以太坊为首的新一代区块链系统试图完善比特币的合约层。比特币尽管也包含了脚本代码，但是并不是图灵完备的，即不支持循环语句；以太坊在比特币结构的基础上，内置了编程语言协议，从而在理论上可以实现任何应用功能。如果把比特币看成是全球账本的话，那么就可以把以太坊看作是一台“全球计算机”——任何人都可以上传和执行

任意的应用程序，并且程序的有效执行能够得到保证。

（六）应用层

应用层则封装了区块链的各种应用场景和案例。比如搭建在以太坊上的各类区块链应用就是部署在应用层，所谓可编程货币和可编程金融也将会搭建在应用层。

该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识机制的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。其中数据层、网络层和共识层是构建区块链应用的必要因素，否则将不能称为真正意义上的区块链。而激励层、合约层和应用层则不是每个区块链应用的必要因素，有部分的区块链应用并不完整地包含着这三层结构。

六、区块链的共识机制

区块链通过数学共识机制是非对称加密算法，即在加密和解密的过程中使用一个“密钥对”，“密钥对”中的两个密钥具有非对称的特点：一是用其中一个密钥加密后，只有另一个密钥才能解开；二是其中一个密钥公开后，根据公开的密钥其他人也无法算出另一个密钥。在区块链的应用场景中，一是加密时的密钥是公开的、所有参与者可见的（公钥），每个参与者都可以用自己的公钥来加密一段信息（真实性），在解密时只有信息的拥有者才能用相应的私钥来解密（保密性），用于接收价值。二是使用私钥对信息签名，公开后通过其对应的公钥来验证签名，确保信息为真正的持有人发出。非对称加密使得任何参与者更容易达成共识，将价值交换中的摩擦边界降到最低，还能实现透明数据后的匿名性，保护个人隐私（如图1.4所示）。

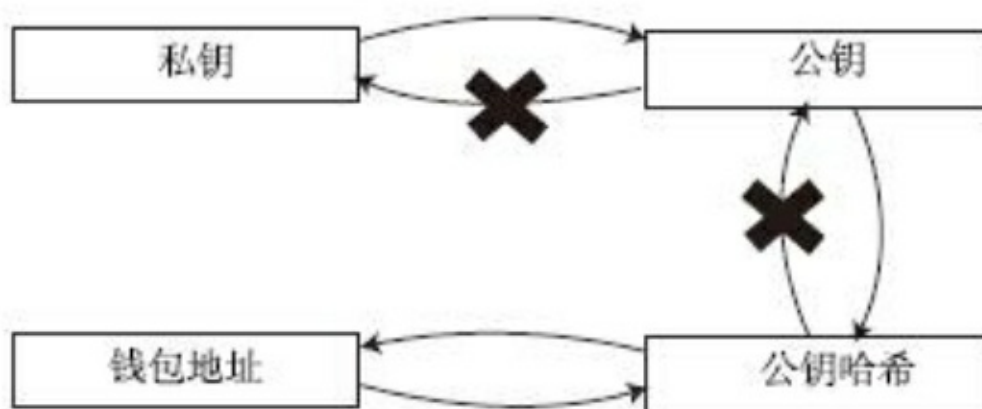


图1.4 私钥、公钥间的关系

资料来源：巴比特、兴业证券研究所

（一）工作量证明机制

所谓工作量证明机制，是指一方（通常为证明者）提交已知难以计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完成了大量的计算工作。

现代最早工作量证明应用是亚当·巴克（Adam Back）于1996年提出的以基于SHA256的工作量证明为反垃圾邮件手段的“Hashcash”（哈希现金）。系统通过要求所有邮件发送时都必须完成大强度的工作量证明，这将使垃圾邮件发送者发大量电子邮件变得很不划算，却仍允许用户们在需要时向其他用户正常发送邮件。现在比特币为了同样的目的使用了一个类似它的系统，而Hashcash的算法也已经被改造为以“挖矿”为形式的比特币安全的核心。

比特币在区块链的生成过程中使用了PoW机制，一个符合要求的Block Hash（区块链散列值）由N个前导零构成，零的个数取决于网络的难度值。要得到合理的Block Hash需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的Block Hash值，说明该节点确实经过了大量的尝试计算。当然，这并不能得出计算次数的绝对值，因为寻找合理的Hash是一个概率事件。当节点拥有占全网n%的算力时，该节点即有n/100的概率找到Block Hash。

PoW看似很神秘，其实在社会中的应用非常广泛。例如，一个人具有的一些技能，如外语口语、乐器或是运动技巧，通常也是一种工作量证明。不用检查四、六级证书，一个人就能流利地说外语或者演奏乐器，那么他一定在这些技能上投入了足够的工作量，而且这个工作量与技能的熟练程度是呈正相关的。如四、六级证书，一般认为在不能作弊的考试里采用足够多的客观题，也可以做到证明工作量的效果，因为一个人从概率上不可能连续蒙对大量的客观题。因此一般认为文凭也是有说服力的。同样地，飞行员的飞行小时数也说明问题，如果你飞了一万

小时还活着，大概就不是靠运气。

在一些其他场合也可以见到PoW的踪影，比如电子游戏里的胜率、K/D比率，在大量的交战中一定的胜率能说明玩家的实力。同样有些游戏里的成就系统、装备体系也是PoW，一般认为成就点数高的玩家在游戏里投入更多，更不容易诈骗，有时候交易点卡要求装备等级或者成就点数也是这个道理。

有些人认为这一方法存在缺陷，即工作量证明浪费资源，截至2016年4月，比特币网络的算力达到1300PHS，即每秒完成13331兆亿次SHA256运算，而最终这些计算没有任何实际意义或科学价值。美国科技网站Vice曾撰文认为这种方式非常不环保，由于多方面原因，比特币网络消耗的能源正日益增长。在最不乐观的情况下，到2020年，比特币网络的耗电量将达到丹麦整个国家的水平。

但是也有观点认为由于需要巨大的投入，促使攻击比特币区块链将会是异常艰难的事情，从而确保了比特币巨大的安全特性，同时也是人类目前构建的最安全的数据库。

（二）权益证明机制

权益证明机制是一种SHA256的替代方法，从根本上解决了工作量计算浪费的问题，它不要求证明者完成一定数量的计算工作，而是要求证明者对某些数量的钱展示所有权，通过每一笔交易销毁的币天数（coin days）来实现，币天数代表一个特定的币，距离最后一次在网络上交易的时间。在给定的时间点内，只存在有限币天数，它们在那些长期持有大量货币结余的人手中持续增加。所以币天数可被视为在网络中权益的代表（proxy，代理服务器）。每当这些币有交易时，币天数即被销毁，因此不能被重复使用。

简单地说，PoS就是把PoW由算力决定记账权变成由持有币数（以及持有的时间）来决定记账权。在PoW中，是按照算力占有总算力的百分比，从而决定你获得本次记账权的概率。在PoS中，持有币数占系统总币数的百分比（包括你占有币数所持有的时间），决定着获得本次记账权的概率。

这就类似于现实世界中的股票制度，在一个公司中，大家是按照持股比例来获得分红，持有股权相对较多的人获得更多的分红权。这种安全机制的理由在于利益捆绑，即大股东比小股东更加关注系统的安全性，所以发动攻击的话，大股东损失更加惨重。在这个模式下，不持有PoS的人无法对PoS构成威胁。PoS的安全取决于持有者，与其他任何因素无关。

反对者认为PoS会加大整个系统中的贫富差距，持有更多币的人更容易挖到新币，即持有股份更多的人会获得更多的分红，从而导致系统内贫富差距拉大。但是，拥护者认为，区块链没有理由去解决系统内的贫富差距问题，而且股份持有者获得相同比例的分红也是现实世界中的原则，并没有人对此有太多的异议。并且在PoW中，那些拥有矿机更多、算力更大的人，也将获得更多的币，因此，PoW也同样存在这样的问题。

（三）股份授权证明机制

DPoS是一种新的保障区块链网络安全的算法。它在尝试解决比特币采用PoW以及PoS问题的同时，还能通过实施去中心化的民主方式，用以抵消中心化所带来的负面效应。

在系统中，每个币就等于一张选票，持有币的人可以根据自己持有币的数量，来投出自己的若干张选票给自己信任的受托人。这些受托人

可以是对系统有贡献的人，也可以是投票者所信赖的人，并且受托人并不一定需要拥有最多的系统资源。投票可以在任意时间进行，而系统会选出获得投票数量最多的101人（也可以是其他数量）作为系统受托人，他们的工作是签署（生产）区块，且在每个区块被签署之前，必须先验证前一个区块已经被受信任节点所签署。

这种共识机制模仿了公司的董事会制度，或者是议会制度。能够让数字货币持有者将维护系统记账和安全的工作交给有能力有时间的人来专职从事该项工作。由于受托人进行记账也能够获得新币的奖励，所以他们会努力拉票，并且维护好与投票者的关系及试图通过参与系统的发展，从而吸引更多人给他投票。

这解决了PoW中的一个主要问题，即在比特币的PoW系统中，持有比特币的人对于系统没有发言权，他们不能参与记账决定权，也不能左右系统的发展，因为系统发言权主要掌握在矿工和开发者手中。而如果矿工或者开发者做出了对比特币持有者不利的决定，比特币持有者除了自己离开系统之外，没有任何可以做的。而在DPoS中，持有者对于记账者拥有足够的选举权，任何试图对系统不利或者作恶的人都随时可能被投票者从受托人的位置直接拉下。

DPoS另外一个巨大优势就是由于记账人数量可控，并且轮流进行记账，能够通过提供更好的软硬件环境来构建效率极高的区块链系统。目前看来，DPoS似乎是效率最高的区块链系统，在理想环境下，能够实现每秒数十万笔的交易数量。

（四）混合证明机制

由于不同共识证明机制有着不同的优劣势，有些系统选择采用多种共识机制的方式来取长补短。较为典型的就是以太坊采用了PoW+PoS的

共识机制。

七、区块链的类型

（一）公有链

所谓公有链，是指全世界任何人都可以在任何时候加入、任意读取数据，任何人都能发送交易且交易能获得有效确认，任何人都能参与其中共识过程的区块链——共识过程决定哪个区块可被添加到区块链中和明确当前状态。作为中心化或者准中心化信任的替代物，公有链的安全由“共识机制”来维护——“共识机制”可以采取PoW或PoS等方式，将经济奖励和加密算法验证结合了起来，并遵循着一般原则：每个人从中可获得的经济奖励与对共识过程做出的贡献成正比。这些区块链通常被认为是“完全去中心化”的。

在公有链中，程序开发者无权干涉用户，所以区块链可以保护使用他们开发的程序的用户。从传统的经济学角度来看，的确难以理解为何程序开发者会愿意放弃自己的权限。然而，随着互联网崛起，协作共享的经济模式为此提供了两个理由：借用托马斯·谢林（Thomas Schelling）的话，即妥协是一种力量。首先，如果你明确地选择做一些很难或者不可能的事情，其他人会更容易信任你并与你产生互动，因为他们相信那些事情不大可能发生在自己身上。其次，如果你是受他人或其他外界因素的强迫，无法去做自己想做的事，你大可说句“即使我想，但我也没有权力去做”的话语作为谈判筹码，这样可以劝阻对方不要强迫你去做不情愿的事。程序开发者们所面临的主要压力或者风险主要是来自政府，所以说“审查阻力”便是公有链最大的优势。

（二）私有链

所谓私有链，是指其写入权限由某个组织和机构控制的区块链。读取权限或者对外开放，或者被进行了任意程度的限制。相关的应用可以包括数据库管理、审计甚至是一个公司，尽管在有些情况下希望它能有公共的可审计性，但在很多的情形下，公共的可读性似乎并非是必需的。

大多数人一开始很难理解私有链存在的必要性，认为其和中心化数据库没有太大的区别，甚至还不如中心化数据库的效率高。事实上，中心化和去中心化永远是相对的，私有链可以看作是一个小范围系统内部的公有链，如果从系统外部来观察，可能觉得这个系统还是中心化的，但是以系统内部每一个节点的眼光来看，其实当中每个节点的权利都是去中心化。而对于公有链，从某种程度来看也可以看作是地球上的私有链，只有地球人的电脑系统才可以接入。因此，私有链完全是有其存在价值的。

私有链的巨大优势就是，由于对于P2P这样的网络系统而言，系统内部的处理速度往往取决于最弱的节点，而私有链所有的节点和网络环境都是完全可以控制的，因此能够确保私有链在处理速度方面远远优于公有链。

私有链和公有链另外一个巨大的区别就是，一般公有链肯定在内部会有某种代币（token），而私有链却是可以选择没有代币的设计方案。对于公有链而言，如果要想让每个节点参与竞争记账，必定需要设计一种奖励制度，鼓励那些遵守规则参与记账的节点。而这种奖励往往就是依靠代币系统来实现的。但是对于私有链而言，基本上都是属于某个机构内部的节点，对于这些节点而言，参与进行记账本身可能就是该组织或者机构上级的要求，对于他们而言本身就是工作的一部分，因此并不是一定需要通过代币奖励机制来激励每个节点进行记账。所以，我们也可以发现，代币系统并不是每个区块链必然需要的。

因此，考虑到处理速度及账本访问的私密性和安全性，越来越多的

企业在选择区块链方案时，会更多地倾向于选择私有链技术。

（三）联盟链

联盟链（Consortium Blockchain），是指其共识过程受到预选节点控制的区块链。例如，可以想象一个由15个金融机构组成的共同体，每个机构都运行着一个节点，而且为了使每个区块生效需要获得其中10个机构的确认。区块链可能允许每个人都可读取，或者只受限于参与者和走混合型路线，例如区块的根哈希及其API（应用程序接口）对外公开，API可允许外界用作有限次数的查询和获取区块链状态的信息。这些区块链可视为“部分去中心化”。比如R3 CEV就是一个典型的联盟链系统。

（四）许可链

许可链（Permissioned Blockchain），是指每个节点都是需要许可才能加入的区块链系统，私有链和联盟链都属于许可链。

（五）混合链和复杂链

随着区块链技术变得越来越复杂，区块链的技术架构开始不仅仅简单地分为公有链、私有链等架构，而是这之间的界限逐渐开始模糊。在区块链的系统中，不再是所有节点都有着简单的一模一样的权限，而是开始有不同的分工。有些节点可能只能查看部分区块链数据，有些节点能够下载完整的区块链数据，有些节点负责参与记账。而随着系统日益复杂，其中不同的角色，以及不同的权限等级会变得更多。其实我们在

DPoS这样的共识机制中，已经能够看到这种趋势开始出现，并不是每个节点都参与记账，而是获得投票数量最多的受托人（Delegated）才开始进行记账，这样的受托人就是典型的角色划分。如果今后央行采用区块链技术发行人民币，肯定会选择类似于混合链这样的技术。

八、区块链的发展脉络

区块链开始引人注目与比特币的风靡密切相关。直至今日，莱特币、狗狗币等类型的比特币层出不穷，人们对于电子货币的关注已经转向了对区块链的深入研究。区块链强大的容错功能，使得它能够在没有中心化服务器和管理的情况下，安全稳定地传输数据。从诞生到现在，区块链专家梅兰妮·斯沃恩（Melanie Swan）将区块链发展划分为三个阶段：区块链1.0、区块链2.0、区块链3.0。

（一）区块链1.0：以比特币为代表的可编程货币

比特币设计的初衷，是为了构建一个可信赖的、自由、无中心、有序的货币交易世界，尽管比特币出现了价格剧烈波动、挖矿产生的巨大能源消耗、政府监管态度不明等各种问题，但可编程货币的出现让价值在互联网中直接流通交换成为可能。可编程的意义是指通过预先设定的指令，完成复杂的动作，并能通过判断外部条件做出反应。可编程货币即指定某些货币在特定时间的专门用途，这对于政府管理专款专用资金等有着重要意义。

区块链是一个全新的数字支付系统，其去中心化、基于密钥的毫无障碍的货币交易模式，在保证安全性的同时也大大降低了交易成本，对传统的金融体系可能产生颠覆性影响，也刻画出一幅理想的交易愿景——全球货币统一，使得货币发行流通不再依靠各国央行。区块链1.0设置了货币的全新起点，但构建全球统一的区块链网络却还有很长的路要走。

（二）区块链2.0：基于区块链的可编程金融

数字货币的强大功能吸引了金融机构采用区块链技术开展业务，人们试着将“智能合约”加入区块链形成可编程金融。目前，可编程金融已经在包括股票、私募股权等领域有了初步的应用，包括目前交易所积极尝试用区块链技术实现股权登记、转让等功能；华尔街银行通过联合打造区块链行业标准，提高银行结算支付的效率，降低跨境支付的成本。

目前商业银行基于区块链的应用领域主要有：一是点对点交易。如基于P2P的跨境支付和汇款、贸易结算以及证券、期货、金融衍生品合约的买卖等。二是登记。区块链具有可信、可追溯的特点，因此可作为可靠的数据库来记录各种信息，如运用在存储反洗钱客户身份资料及交易记录上。三是确权。如土地所有权、股权等合约或财产的真实性验证和转移等。四是智能管理。即利用“智能合同”自动检测是否具备生效的各种环境，一旦满足了预先设定的程序，合同会得到自动处理，比如自动付息、分红等。目前，包括商业银行在内的金融机构都开始研究区块链技术并尝试将其运用到实践中，也许现有的传统金融体系正在逐渐被区块链技术所颠覆。

（三）区块链3.0：区块链在其他行业的应用

除了金融行业，区块链在其他领域也开始应用。在法律、零售、物联、医疗等领域，区块链可以解决信任问题，不再依靠第三方来建立信用和信息共享，提高整个行业的运行效率和整体水平。极高的生产力会将这个地球上所有的人和机器连接到一个全球性的网络中，人类向商品和服务近乎免费的时代加速迈进，也许到了21世纪下半叶，资本主义走向没落，区块链的去中心化协同共享模式将取而代之，成为主导经济生活的新模式。

区块链是这种新兴协同共享模式的最佳技术手段。区块链的基础设施以去中心化的形式配置全球资源，使区块链成为促进社会经济发展的理想技术框架。区块链的运营逻辑在于能够优化点对点资源、全球协作和在社会中培养并鼓励创造社会资本的敏感程度。建立区块链的各类平台能够最大限度地鼓励协作型文化，这与原始共有模式相得益彰，将使其成为21世纪决定性的经济模式。

现在我们所说的区块链1.0、区块链2.0、区块链3.0，也许感觉这是一种递进的演化，但事实上仅仅是应用范围的不同而已，从区块链1.0到区块链3.0都是平行的发展阶段，在各自的领域内发挥应有的作用。通过区块链技术，能够让人类生活在许多应用和工具中，进入“可编程”状态和智能状态，完成非常复杂的操作。

20世纪90年代，信息技术的飞速发展变革了现代社会，数据计算、数据库应用等为互联网技术应用打下了基础，在深度和广度拓展了人们的世界观。人们从对比特币的关注，到区块链技术在金融领域大显身手，进入2015年，区块链建立去中心化信用的尝试，已经不限于金融界，而被社会各个领域关注，特别是在中国，目前社会的公信力普遍不足的情况下，区块链更能为社会管理提供一种全新的思路和技术选项。比特币的成功和金融领域的尝试性运用，使社会对区块链的关注度和投资热度急剧提升，区块链技术的发展进入黄金时期。

区块链飞速发展描绘了世界基于技术的统一愿景，整个社会有望进入智能互联网时代，形成一个可编程的社会。在这个信用已经成为紧缺资源的时代，区块链的技术创新作为一种分布式信用的模式，为全球市场的金融、社会管理、人才评价和去中心化组织建设等提供了一个广阔的发展前景。

第二章 智能合约

智能合约是能够自动执行合约条款的计算机程序。未来某天，这些程序可能取代处理某些特定金融交易的律师和银行。区块链之所以被认为是一种颠覆性的技术，主要就是因为区块链上能够实现智能合约。

智能合约的潜能不只是简单的转移资金。一辆汽车或者一所房屋的门锁，都必须被链接到物联网上的智能合约才能被打开。但是与所有的金融前沿技术类似，智能合约的主要问题是：它怎样与我们目前的法律系统相协调呢？会有人真正使用智能合约吗？

一、什么是智能合约

智能合约的理念可以追溯到1994年，几乎与互联网同时出现。曾经为比特币打下基础，从而备受广泛赞誉的密码学家尼克·萨博（Nick Szabo）首次提出了“智能合约”（smart contract）这一术语。他对于智能合约的定义是：“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。”

从本质上讲，这些自动合约的工作原理类似于其他计算机程序的if-then语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约便执行相应的合同条款。

这里的“智能”，在英语中对应的单词是“smart”，而不等同于“人工智能”（Artificial Intelligence, AI）。Smart代表的意思是聪明的，能够灵活多变的，但还没有能够达到“人工智能”这样的级别。所以有些人仅仅从中文字面上理解，认为必须要达到“人工智能”才能算是智能合约，其实就和“智能手机”一样，这里的“智能”仅仅是指可以灵活定义和操作。

二、智能合约的三要素

萨博关于智能合约如何工作的理论，到目前为止在实践中还没有实现，因为直到今天，还没有天生能够支持可编程交易的数字金融系统。因为，如果银行仍然需要手动批准资金的转移，那么智能合约的目标就无法实现。所以，可以认为，实现智能合约的一大障碍是现在的计算机程序不能真正地触发支付。

而比特币的出现及广泛应用，正在改变阻碍智能合约实现的现状，从而让萨博的理论有了重生的机会。智能合约技术现在正建立在比特币和其他数字货币——有些人将它们称为区块链2.0平台之上。因为大多数基于区块链技术的数字货币本身就是一个计算机程序，智能合约能够与之进行交互，就像它能与其他程序进行交互一样。所以，随着区块链技术的诞生，这些问题正逐步被解决，已经可以通过计算机程序来触发支付。

类似于比特币基于区块链技术的密码学数字货币已经准备就绪，能够帮助智能合约成为现实，而最终将可能会实现数字货币和智能合约的双赢。智能合约能够向人们说明数字货币独特的益处，而这将为数字货币吸引更多的用户。从这一点来看，也许智能合约就是数字货币的真正“杀手级应用”。

在区块链的环境下，合约或者智能合约意味着区块链交易将会远不只简单的买卖货币这种交易，还将会有更加广泛的指令可以嵌入区块链中。在更正式的定义中，一个合约就是通过区块链使用比特币和某人形成某种协议。

传统意义上的合约，就是双方或者多方协议做或不做某事来换取某些东西。合同中的任何一方必须信任彼此并履行义务。智能合约的特点

是，同样是彼此之间同意做或者不同意做某事，但是无须再信任彼此。这是因为智能合约不但是由代码进行定义的，也是由代码（强制）执行的，完全自动而无法干预。

事实上，首先，智能合约之所以如此是因为三个要素：自治、自足和去中心化。自治表示合约一旦启动就会自动运行，而不需要它的发起者进行任何的干预。其次，智能合约能够自足以获取资源，也就是说，通过提供服务或者发行资产来获取资金，当需要时也会使用这些资金。最后，智能合约是去中心化的，这也就是说它们并不依赖单个中心化的服务器，而是分布式的，通过网络节点来自动运行。

用一个形象的说法来比喻智能合约，即可以把它看成由代码编写的且能自动运行的自动售卖机。不同于人的行为，一台自动售卖机的行为是可以计算的；相同的指令行为总是会得到相同的结果。当你塞入一些钱并做出选择后，你选择的物品就会掉出。机器绝不可能违反预定程序来执行，也不会仅仅执行一部分（只要它没有被损坏）。一个智能合约也同样是如此，一定会按照预先设定的代码来制定。在区块链和智能合约的世界中，“代码即法律”，无论怎么编写，它都会被执行。在某些情况下，这可能是好事也可能不是；无论是与不是，都将会是一种全新的情况，我们的社会在智能合约普及之前还有一段较为漫长的适应阶段。



图2.1 智能合约三要素

基于加密算法的智能合约及其相关体系，如果要能够激活资产还有许多细节需要考虑。也许我们还需要全新的法律和相关规定，来区别于那些通过代码来建立的合约与通过人来建立的具有司法约束力的合同之间的异同。只有基于通过人来约定建立的合同才会有遵守或者违反合同的情况，而基于区块链以及任何基于代码的合同都不存在这样的问题。此外，智能合约将不仅仅会影响到合同法，而且可能会影响整个社会中的其他社会性契约。

需要确定和界定何种社会契约会更需要“代码法律”，即根据代码来自动执行且无法阻止运行。因为基于目前所颁布施行的法律，几乎不可能让智能合约强制执行（例如，一个去中心化的代码样本在事后是难以控制、监管或者要求赔偿损失），在现有法律框架本质上要把这种行为下降到人为合同的水平。最终的目标将不是没有法律或者是无政府状态，而是让法律框架变得根据具体情况而更加精细化和个性化。各方可以通过协商来选择某个法律框架来建立一个合同然后将它写入代码中。这样根据大家都已经知道的、审核过的且“陈旧”的法律框架，类似于创作共用许可证（Creative Commons Licenses），这样用户可以选择某个法律框架作为智能合约的框架。因此，可能会有许多类型的法律框架，就像会有许多货币一样。

智能合约并不是意味着能够实现一切所不能做到的事情，事实上，它们能够以最大限度地减少信任的方式来解决一些普通事情。最小化信任能够让事情变得更加便捷，因为其通过全自动执行替代了人的自主判断。

三、智能合约的范例

（一）博彩交易

让我们举一个简单的例子，以超级碗比赛为例。假如你赌Patriots（新英格兰爱国者队）赢，下注500美元，或者一个比特币，你的朋友赌Packers（绿湾包装工队）赢，下同样的注。第一步，你和你的朋友将你们的比特币发送到一个由智能合约控制的中立账户。当比赛结束时，智能合约能够通过ESPN（娱乐与体育节目电视网），路透社或者其他媒体确认Patriots战胜了Packers，智能合约将自动地将你的赌金和从朋友那里赢得的钱发送到你的账户。

因为智能合约是计算机程序，所以很容易增加更加复杂的赌博元素，例如赔率和分差。尽管现在有处理这种交易的服务，但是都会收取相应费用。智能合约与这些服务的不同之处在于，智能合约是一个任何人都可以使用的去中心化的系统，不需要任何中介机构。

（二）网络购物

一个更加常见的例子是网上购物。如果你从网上购买了某物品，你可能不想立即付款，想等到卖家发货后再付款。所以你可以很容易地创建一个合约，该合约通过查询顺丰速运的物流数据，智能合约只有确认你购买的商品已经发往你的地址时，才发送货款给卖家。这样，是不是可以发现，我们所用的支付宝的中介功能也可以被程序自动替代？

（三）抵押贷款

还有许多常规的金融交易，律师和银行的工作归根到底是重复性地处理平凡的任务。但是我们还不得不向律师提供管理遗嘱或者向银行提供抵押贷款的工作支付大量的报酬。而智能合约能够使得这些处理过程自动化和非神秘化，节省人们的时间和金钱。

尽管可以通过一家银行获得抵押贷款，但是一般而言，银行不会持有长达30年的贷款，这些抵押贷款将被转移给投资者。但是，你继续向银行还款，而不是持有你的贷款的投资者。银行只是你每月还款的处理者，向投资者支付其中的大部分，小部分缴税，更小部分用于房主的保险。这其实只是一个非常简单的操作任务，但是银行经常需要一个季度到半年的时间来处理抵押贷款的还款问题。他们只是从贷款者手里接收还款，将还款转交给投资者，只是凭此服务来向人们收费。然而，理论上，智能合约能够非常容易地处理这种业务。如果贷款还款由智能合约处理，那么贷款处理费用将被取消，省下来的钱可以给消费者，最终的结果是获得房屋所有权的成本更低。

（四）遗产分配

虽然智能合约仍处于初始阶段，但是其潜力显而易见。想象一下分配遗产的场景，通过智能合约会让决定谁得到多少遗产这件事变得非常简单。如果开发出足够简单的用户交互界面，它就解决许多法律难题，例如更新你的遗嘱。就像赌博或者顺丰速运的例子，一旦智能合约确认触发条件——你已经死亡——合约就将开始执行，你的财产将被立即分割。

或者当某个孙辈到了18岁或者祖父母死亡的某天，通过智能合约执行继承财产。这个交易事件可以写入区块链中，而到未来某个事件发生

或者到未来某个时间点时，交易被触发。需要设置的第一个条件——孙辈在18岁时收到一份继承资产，程序需要设置执行交易的具体日期，包括还要检查该项交易是否已经被执行。还需要设置的第二个条件——程序需要扫描一个在线的死亡登记数据库，或预先指定的某个在线报纸的讣告区，也可能是某种“预言”信息来证明祖父辈已经过世。当智能合约确认了死亡信息，它就能够自动发送资金。

（五）物理世界

想到用智能合约管理遗嘱并不难。如果你能想象你的所有资产都是比特币，用智能合约管理遗嘱的方式就可行。但是，如果你像我们大多数人一样，生活在物理世界中，拥有实体资产，那该怎么办呢？智能财产也可以解决这些问题。

物联网正在不断发展，每天都有越来越多的智能设备连接到网络上。一些思想超前的开发者已经开始着手将物联网和区块链技术结合在一起，所以像许多基于区块链的数字货币或者数字资产实际上就可以代表一个物体。这种通常以代币形式出现的就是所谓的智能财产（smart property）。

但是比代表一些物体更为重要的是，这些新的智能财产代币实际上允许取得对一个联网物体的控制权和所有权，无论它是一台电脑、一辆汽车还是一所房子。

让我们先释放一下想象力，假设所有的门锁都是连接在互联网上的。当你为租房进行了一笔数字货币交易时，你我达成的智能合约将自动执行为你打开房门。你只需要用存储在智能手机中的钥匙就能进入房屋。并且，一个智能合约也将使得当这些数字钥匙到期时，设置日期更加容易。这听起来有点像已经不需要Airbnb（空中住宿）的私人房屋出

租服务。

如果你考虑到这一点，这就是智能合约追求的根本性变革。Airbnb提供的服务被人们需要的原因是，它使得房东和租房者不需要互相信任彼此——他们只需要信任Airbnb。如果租房者不向房东付钱，或者房东不给租房者钥匙，他们都可以上诉到Airbnb来解决。

使用智能合约进行房屋出租，将取代像Airbnb这样的商业模式。房东和租房者仍然不需要信任彼此——他们只需要信任智能合约。智能合约将使得以前需要信任的商业模式去中心化。如此一来，它将消除像Airbnb这样的中介所收取的高额费用。

智能合约不仅能颠覆现有的商业模式，它们也能够完善现有的商业模式。萨博在他1994年的论文中已经预想到了“智能财产”，并写道：“智能财产可能以将智能合约内置到物理实体的方式，被创造出来。”他举的一个例子是汽车贷款，如果贷款者不还款，智能合约将自动收回发动汽车的数字钥匙。毫无疑问，智能合约这种用途对未来的汽车经销商很有吸引力。

四、智能合约的应用案例

Visa（维萨卡）正在努力使用全新的区块链技术来彻底变革汽车购买和使用流程。希望购买一辆车很快就会变得和网上订购一个比萨那么简单。

这个原型应用程序已经在2015年10月拉斯维加斯召开的Money 20/20支付会议上进行了介绍，正在DocuSign实验室里被开发中。试想一下，如果你走进一家汽车销售店，并且你已经知道了自己想要的汽车、颜色以及在选择范围之内两三个特性。随着手指的轻触和滑动，在选择了每年的里程之后，一个客户就可以直接从销售店租借出一辆车，整个过程不到五分钟。而这一切仅仅是开始。

Visa和DocuSign的工程师们通过创建的APP（手机软件）能够让你同样快速和简单地购买汽车保险。不需要更多的传真文档，以及数小时来等待保险员处理。随着DocuSign独有的数字交易管理平台和电子签名，并且集成了Visa支付技术的发展，汽车将能够在比特币区块链上进行车辆登记。

类似于Visa把信用卡技术集成进入苹果手表（提供Apple Pay的手腕支付方式，Apple Pay即苹果支付），这就如同把信用卡放入到你的车辆中。车辆能够成为一种智能资产，并且为方便消费者实现双向通信。

从此，汽车将可以自动完成很多事情，包括支付过路费，购买比萨饼，或者建立一个银行账户。这类应用只要花数个星期来创建，如需要，也可以很快整合到车辆内。这个APP能够监视经销店的折扣情况，当所有者驾驶的里程少于原来约定的里程，还能够重新进行注册、支付停车费，或者是为汽车订购卫星广播等，甚至车辆都可以自己“拥有”自己。

对于车主而言，汽车能够实现的能力似乎变得无穷无尽。你所在的地区，所有和汽车相关的服务都将被集成进去，并且通过APP来竞标为你服务。

汽车4S店的服务人员将会知道你汽车的所有状况，以及在你上路之前汽车需要什么，或者在你家附近的加油站会通过反向竞标来获得你这单生意，当你把车开过去停下来时，你甚至不用掏出你的钱包。

类似于这样的应用程序，显示了在物联网世界中，通过整合电子设备、区块链和智能合约所产生的巨大潜力。根据一些分析师估计，从门锁到相机，可能会有多达500亿个物体连接到网络上，到2020年将有2.5亿辆汽车会接入物联网。

五、智能合约可能面临的威胁

从某种程度上说，智能合约可以成为犯罪行为的完美载体，因为，它要在难以达成信任的情况下创造出信任。也可以尝试举出一些非法的“智能合约”的例子。这些合约就可以在最近上线的智能合约平台上实现。其中的一份合约是，如果某人能够黑掉某个特定网站，那么，他能够获得数字货币的奖励。通过平台，合约的一方可以控制这份奖励，只将其提供给那些有证据完成此项工作的人。

研究人员认为，智能合约可以用于许多形式的犯罪。为此，他们举出了一个更为大胆的例子。例如，某人可以设计一份合约，要求刺杀一个公共人物。如果有人想要酬金，他可以提前提供信息，包括刺杀的时间和地点。然后，当这些细节在可信任的新闻网站得到证实时，酬金会支付给这个人。

智能合约完全有可能被犯罪分子利用，这应该不会让人感到奇怪。做违法生意的人通常首先采用新技术，因为他们没有什么可失去的。与传统的基于现金的犯罪相比，利用比特币或者智能合约的犯罪，在目前看来不会有太大规模。与比特币交易相比，智能合约更为复杂，而且撰写、理解合约都需要特殊的编程技巧。

尽管如此，但这也是新技术令人感兴趣的地方。文件分享上的侵权行为迫使娱乐和科技界做出改变，平台上的违法行为也可能会改变世界。智能合约平台可能对社会产生重大的影响，它可能成为各种社会变化的技术基础。

我们可以想象一下，通过智能合约平台完全可以用于创造去中心化的Uber（优步）服务。这种服务可连接司机和乘客，并且轻易处理支付问题，而不需要中间公司的存在。如果这样的话，反对Uber的执法者会

发现，他们失去了打击的对象。通过智能合约可以实现任何形式的网络服务，背后不需要有法律实体，使某些东西成为法律无法禁止的，这也许是一个非常大胆和危险的想法。

六、智能合约的未来展望

智能合约有利的一面是，它将使得金融机构更加乐意接受穷人带来的风险，如果没有智能合约他们可能得不到贷款。因为，在遇到最坏的情况下，如果某人不能偿还贷款，对银行而言，收回资产并不是件轻而易举的事。

除了增加获得信用贷款的机会外，智能合约也有潜力为没有优势的人打开接触司法系统的大门，没有智能合约，这些人就没法获得应有的收益。智能合约将有利于那些不能支付法律费用的人使用司法系统。

虽然，理论上法律平等地对待每一个人，但当合约的另一方违约时，你到法庭上控告他们是需要的。而现实情况大多如此，只有你能花钱请得起律师执行协议时，正义才能得到伸张。而智能合约是能够自动执行协议的，它将改变原有的游戏规则。

这听起来好像我们将不再需要律师，但是事实上，智能合约应该被视为法律系统的进化，而不是消除。只不过，未来律师的职责可能完全不同于现在。在未来，律师的职责不是裁定个人合约，而是在一个竞争市场上生产智能合约模板。合约的卖点将是它们的质量，即定制性如何，易用性如何。这听起来有点像是一个交易网站模板的市场，但事实上就是如此。以后许多律师将会创建出不同事情的法律智能合约，他们可以将合约卖给其他人使用。所以，如果有律师制作了一个非常完美的、具有不同功能的权益协议，那么就可以收费许可别人使用。

当然，这些合约很有可能是需要通过程序语言来实现的，也就是未来律师的主要工作是会写程序，这对于现在的律师而言，可能是一个非常有趣的挑战。

有一件事确定无疑：智能合约已经扎下根了。它们是全球经济真正的基本构件，任何人都可以接触到这一全球经济，不需要事前审查和支付高昂的预付成本。它们从许多经济交易中，移除了对第三方的信任必要，在任何情况下，将信任转移到可以信任的人和机构。

当然，智能合约在现实中可能不像刚才所说的那样明确。尽管在理论上，智能合约听起来非常美好，但是现在还不可能预测它如何在法庭上起作用。没有律师或者法律仲裁者的愿景十分吸引人，但是我们真的能够冒险用代码法律取代文本法律吗？这些还有待观察。

此外，智能合约是完全可以与现有的《合同法》共存的。本质上，它们是解决相同问题——以一种方式形成一种关系，使得承诺可以执行的两种不同方法。就这一点而言，智能合约似乎是更好的解决方案，即智能合约事前执行，不像法律系统的事后执行。

第三章 DAO和DAC

一、关于DAO和DAC

（一）定义

DAO（Distributed Autonomous Organization，分布式自治组织）和DAC（Distributed Autonomous Corporation，分布式自治机构）也许是自比特币诞生以来，区块链技术基础之上最重要的概念之一。我们相信DAC将会变得越来越重要。

DAO和DAC现在已经被越来越多地提到，甚至还有一个基于区块链投资基金项目的名字就是DAO（这个DAO是项目的名称，和我们现在所说的分布式自治组织没太大的关系）。DAO和DAC这两个概念并没有太大的区别，在早期更多地使用DAC概念，而在2016年，越来越多的人开始使用DAO这个术语。

所谓DAO和DAC，就是通过一系列公开公正的规则，可以在无人干预和管理的情况下自主运行的组织机构。这些规则往往会以开源软件的形式出现，每个人可以通过购买股份或者提供服务的形式获得股份来成为公司的股东。机构的股东将可以分享机构的收益，参与机构成长，并且参与机构的运营。

（二）三定律

在具体实践DAO和DAC时，以下三个定律应该被认真地放入DAO和DAC的系统准则中，并且能够让所有股东检验这三条定律是否得到了严格的执行。通过这三条定律，将可以监控系统中股东权益的保护以及其他的规则如何被更改，但它们自己永远不可以自主更改这些规则。

第一定律：诚信机制。

靠多个DAO和DAC节点来对每一个DAO和DAC节点的行为进行互相审查，来确保所有的规则能够被强制实施。而单个节点的无赖行为则会被集体简单封锁。即使是系统的制造者不遵守规则也是无效的，而有敌意的高压控制也将会是无效的。

第二定律：不可侵犯机制。

能够确保在没有多数股东同意的情况下，对任何DAO和DAC规则（源代码）的更改都是不被执行的，没有集体一半以上的投票来同意采纳，对极少数节点的侵犯也是不会成功的。

第三定律：自我保护。

能够让整个系统采取更多的手段，以抵挡对DAO和DAC生存造成任何威胁因素的能力。前两个定律已经降低了引入坏的节点的可能。一个公开的系统或者是开源软件，能够通过上述手段来避免由于引入不良节点而造成整个系统崩溃的可能。

（三）简单模型

我们可以设想建立一个DAO和DAC化的微博，这个微博系统没有中央化服务器，而是提供一个客户端（网络客户端、软件也可能包括APP）。该微博DAO和DAC会提供和新浪微博类似的微博功能，每个人

可以在系统中免费发布微博，系统每10分钟将最新微博打包后，将微博信息整理后放入区块链的新块中，而这个新块会发送到各个节点中。许多新的参与者贡献自己的计算机和硬盘当作系统中的一个节点，作为回报，系统会给提供算力和硬盘的节点以微博币（简称为WBB，WBB开始每小时发送100个，以后每年减半），每个微博币将自带一个比特币地址。而系统除了提供发布微博功能，也会提供一些特殊的收费功能，比如可以将微博置顶或者在微博进行一定范围的广播，而这些功能每次使用时，需要支付0.0001比特币。另外，还提供广告接口，需要在微博中发布广告的广告商需要预先向系统支付一定的广告费用（通过内置的比特币地址），然后按照点击量或者浏览数，系统会自动扣除相应的比特币。而系统每24小时，会将所收取的比特币，以当前已经发放的WBB总量，发送到持有WBB的个人账户中。

这样，就构建了一个简单的微博DAO和DAC，在这个DAO和DAC中，一开始也许参与的人不太多，很可能在小范围内进行交流，但如果开发团队对这个DAO和DAC有着很大的信心，可以在最初发布后，自己成为节点开始挖矿，然后不断地进行优化和推广，只要该微博开始有一定的收入，就会有人加入系统成为节点，来获得WBB以获得相应的回报。同时由于每个WBB本身具有能够获得比特币的功能，这就意味着市场将会对WBB本身有一个估值，而每个WBB也将可以自由交易。随着WBB估值越来越高，会有越来越多的人贡献自己的算力和硬盘，而由于用户体验越来越好，也会有更多的人使用微博。由此便可以形成一个良性的循环。

整个微博DAO和DAC是完全开源的系统，同时它也是完全去中心化的，这就意味着该微博DAO和DAC将处于比较难以被攻击和监管的位置。简单的电子商务DAO和DAC模型也可以构建一个类似于淘宝的电子商务DAO和DAC。同样也是让买卖双方进行交易，当然一开始这个DAO和DAC可能只能接受比特币作为唯一货币。然后系统将会从交易中收取1%的手续费，然后同样按照比例发放给系统提供计算力和数

据存储的节点。同样，它也可以发放某种数字货币作为对于贡献的标识，而这个数字货币可能接近于公司的股份。事实上，目前已经有了Openbazaar这样的去中心化的电子商务系统，在后面的章节我们会详细介绍它的模型。

显而易见，这样的DAO和DAC也是全球化、去中心化进行发展。而整个系统也能够构建一个良性循环并且对于每个参与者都有着持续贡献自身能力的驱动力。

而对于非DAO和DAC而言，如果让你参与到像淘宝这样的项目是非常困难的，但是对于DAO和DAC而言，每个人都可以随时参与，并且随时根据自身的能力来选择投入的资源 and 精力。通过DAO和DAC，很多原本没有任何交集的人都可以抱着同样的目的进行协作。他们之间可能永远都不认识，但是却可以为了同一个DAO和DAC而付出努力，并且伴随DAO和DAC的成长获得相应的回馈。如果没有DAO和DAC，这在过去是难以想象的。

（四）未来

前文仅仅举了两个很简单的设计模型，其实在虚拟空间或者现实社会中能够找到的所有模型（无论是商业还是非商业的），似乎都有可能进行DAO和DAC化，这取决于设计者的奇思妙想，即是否能够构建出一个自我监督并且自我完善和发展的DAO和DAC体系。当然，可以预料到DAO和DAC能够变得越来越复杂，甚至其结构远远超出我们现在的想象范围。

感谢区块链技术带来的革命，使DAO和DAC的成功变得如此真实。这并不只是用于数字货币，这是建立几乎所有种类的不可侵犯的商业关系的一种方法，采用这种新的方式所带来的不同，就像是选择平面

还是球体作为模型来规划你的全球航海线路一样。当我们在吸取以往那些由市场驱动的公司是如何在真实世界里运作的经验时，各种各样的灵感就会产生。在设计时可以分两步走，首先，尽力想象你能设计的一个机器人化的公司实体，它需要的是对客户和股东利益有着不可侵蚀的忠实，那么它应该具有何种价值；其次，让我们考虑如何让它像一个出色的传统公司一样运作，从而能够与善变的人类对手竞争。

只有当软件能做一些有用的事情时，能够彻底诚实且不受情绪影响的软件技术才是有价值的。一个DAO和DAC是一个可以以很多种方式运作的公司，如同那些由砖头和人组成的公司一样真实。因为一个DAO和DAC提供了忠实的有价值的服务，它产生了可以以其股份形式被保存和转让的真实财富。

但也必须知道DAO和DAC的局限性，一个独立自主的DAO和DAC没有办法在不依赖于外力的情况下接受、持有或移交物理商品或法币。一个开源的DAO和DAC无法保守秘密。它可以安全地为他人保有加密数据，但却无法为自己存一把私钥。因此，一个DAO和DAC不能拥有自己的装满数字资产的加密钱包。

二、燃料货币理论

（一）DAO是如何盈利的

由于区块链最显著的特性是去中心化，没有任何中心化的个人或者组织能够完全控制区块链项目，因此很多人都无法理解区块链项目本身是如何盈利的。通常情况下，区块链项目往往就是一个程序，而且是开源程序，这就意味着任何人都可以进行复制和修改。而在所有的区块链项目中，名声最大的是比特币，其创始人尽管拥有巨大的财富，却从来没有现身过，更没有从中获取过任何利益。这许多人都认为，开发区块链项目是不是都是为了兴趣和理想，完全无私奉献的人。对于那些从来没有参与区块链项目，特别是没有参与过除了比特币之外的人，很难去理解为什么有人会去开发区块链技术。

如果这些人都是为了理想而参与，那就让人颇有忧虑，因为一个行业需要得到最广泛的支持，必定需要以商业利益为诉求。而如果没有商业利益来驱动，仅仅是依靠所谓的理想或者兴趣，是很难支撑一个巨大行业向前发展的。

事实上也是如此，比特币创始人中本聪仅仅是一个特例，尽管区块链的许多其他项目的创始人也充满着理想和激情，但他们从来没有否认过自己的商业意图，并且很多人就是为了这个意图而努力奋斗的。

但是开源软件如何赚钱真的是一个令人费解的问题。所谓开源软件，就是源代码开放的软件，任何人都可以下载查看其全部源代码，并且可以在无条件或者有条件的情况下进行修改和重新编译。自从有了程序那一天，应该就有了开源软件，这经常被认为是一种自由的象征，标

志着共享的精神。但是，一般情况下，这也意味着不是商业软件，考虑到商业软件的目标是为了盈利收费，而开源软件既然任何人都可以免费下载和研究，自然没有多少人会为之付费。所以，只要是开源软件一般默认就是非营利性的软件。

区块链项目往往都是开源软件，比特币就是一种典型的开源软件，有许多人可以免费下载，并且也有不少人对它进行修改和重新编译，变成一些全新的其他数字货币软件。大多数其他纯粹的区块链项目也是开源的，既然开源软件天生就和非商业软件联系在一起，难免让很多人对于类似于DAO这样的区块链项目是如何盈利的产生疑问。

但是，事实上就是因为区块链技术的出现，第一次让开源软件有了盈利的途径。这个途径就是燃料货币方式，燃料货币方式开创了软件的全新盈利模式，甚至可能会改变公司盈利的方式。

（二）燃料货币方式

所谓燃料货币理论，就是在一个纯区块链项目，也就是形式类似于DAO和DAC这样的区块链项目中都有一种代币，任何人在使用该项目提供的服务时都会被要求使用这些代币支付一定的费用（往往是较小的数额）。随着使用者越来越多，就会对这些代币产生更多的需求。因为在某一个时刻，代币的数量肯定是有限的（在DAO中，没有任何人能够随意修改代币数量），从而使代币价格升值。而这些代币往往在项目的开发者手中，以及早期的投资者手中。那些开发者为了让自己持有的代币增值，自然就有动力把项目开发得更加完善，来吸引更多的人使用。而那些早期投资者，为了让自己持有的代币增值，也就有动力自愿推广这些项目，让更多的人来使用该区块链项目。因为只要有越多的人来使用该项目，也就能让代币需求越多，从而使得开发者和早期投资者获利。如此看来，每次支付一定的费用来让系统提供一定的服务，有些像

给汽车加油，汽车不断地运行的前提是需要不断添加像汽油这样的燃料。所以，一般将这种方式称为燃料货币方式。

正是由于燃料货币方式的出现，基于区块链技术的开源软件也能够使开发者和投资者盈利，只不过不同于传统的卖软件或者卖许可证的方式，而是必须以让更多的人使用为前提，让最初的开发者有动力不断地提升整个系统的质量，而投资者也有动力成为一个义务的销售者，努力地推广该系统的使用范围。从这一点来看，这已经完全构成了一个正向循环。

以太坊就是燃料货币方式的典型案例。我们可以把以太坊想象成区块链世界中，类似于Windows（视窗操作系统）和Android（安卓）这样的底层操作系统。而在以太坊中的许多计算机组成的节点来负责进行各种智能合约的计算。在以太坊之上，会搭建各种各样的应用，而这些应用在执行各种任务，提供各种服务时就需要调用以太坊底层的计算资源来执行智能合约。那些提供计算服务的节点并不是免费的，他们是要收取费用的，收取的就是以太坊的代币——以太币（Ether），因此那些使用调用资源应用的用户就需要支付以太币。在以太坊中，许多以太币就在那些以太坊开发者，以及早期投资者手上（以太坊是通过众筹来获得早期资金的，他们按照投资者参与众筹的资金，按比例发送一定数量的以太币）。在以太坊中，这种用于获得服务而支付的代币就被称为Gas（汽油）。

在以太坊上搭建的应用越多，那些自然应用所调用的资源也就越多，从而需要支付的以太币需求也就越大，从而必然会造成以太币需求越来越大，使得在市场上流通的以太币的价格越来越高。从以太坊发布第一天开始，截至目前，尽管以太币价格一直在波动，但是的确能发现，随着以太坊得到越来越多的认可，以太币价格也在逐步升高。

比特币也是类似于这样的方式，在传输比特币时，如果支付极小数量的比特币，就能够提高比特币交易确认的速度。从这一点来看，这种

方式也算是一种通过支付费用来获得快速交易的服务。但是，比特币作为一种支付手段，它本身提供的服务就是把自身（比特币）进行传输，那么只有使用比特币的人群越来越大，对于比特币本身需求才会越大，从而才能造成比特币价格的不断升高。每个比特币从最早的不到一美元，到今天价值数百美元（截至2016年5月，其价格在400美元左右进行浮动），很大一部分原因也是对比特币需求变得越加广泛。尽管我们相信比特币的创始人中本聪应该是一位不在意金钱的君子，但是他持有的那些比特币，却已价值高达数亿美元。

（三）颠覆公司制度

公司是现代商业社会中非常重要的组织形式，是构成现代整个商业社会的基础。尽管目前公司制度已经可以发展为非常复杂的形式，但基本上都可以把公司视为一种通过提供某种商品或者某种服务，从而营利的组织形式。如果从这个定义出发，无论是DAO还是DAC，都可以被视为一种公司，只不过这种公司的内部运作方式已经完全不一样。

我们目前的公司，一般由投资者、管理者、生产者和销售者来构成。投资者用资金投入来创建企业和维持运作，管理者负责指定公司运行规则并维护公司运作，生产者为消费者制造产品或者服务，而销售者把这些产品和服务推广给消费者。消费者支付的费用成为公司的收益，去除公司成本后，剩下的都是公司的利润。而任何人无论是要成为某个企业的投资者、管理者、生产者还是消费者，只要该企业不是只有一个人，一般都必须要经过一些复杂的流程，得到现有其他人的认可，特别是要获得管理者的认同。这是每个加入或者创办过公司的人都非常熟悉的内容。

在区块链的世界，却可以把这一切极度简化。首先管理者消失了，已经变成了能够自动运行的程序，我们可以把这个程序看作预先设定好

的企业公司运作规则，由于DAO都是开源程序，所以这些预先设定的公司规则人人都可以了解。而这段程序由于并不是控制在一个人手上的，而是分布在不同的节点，所以除非大多数人都完全认同，否则这些原则是无法被修改的。

生产者则是那些系统的开发者，他们通过设计不同的应用来为潜在的消费者提供其可能需要的服务。当然，他们也能够通过编写程序来定义各种系统规则，但是不像传统的管理者，这些定义的规则必须得到大部分参与者的认同，否则大家完全可以忽视他们制定的规则，或者重新修改的新规则。所以说，从某种程度而言，他们更接近于提供建议的人，而不是决策者。

投资者仍通过投入资金获得公司的股份，只不过在区块链的世界里，股份以代币的形式出现。所以，我们完全可以把每个比特币视为比特币系统中的股份。不像传统企业那种非常复杂的方式，消费者支付货币来获得某种产品和服务，公司通过获得更多的收入让公司变得越来越有价值，从而使公司股份的价格变得更高。因此，在区块链行业里，消费者直接通过购买企业股份（代币）来获得产品或服务，从而造成股份价格升高。在这个过程中，货币这个环节就直接被忽略了，也让系统变得更加有效率。

同时投资者为了让自己的股份更有价值，也很有可能成为一个义务的销售者，试图通过让更多的消费者购买公司的产品或服务，来让自己的股份变得更有价值。考虑到这些股份可以在很多数字资产交易所进行交易，具有极高的流动性，就等于是已经上市的企业。

于是，我们发现通过DAO和DAC的方式，公司被简化成只有投资者和生产者，而消费者直接通过支付股份来消费，使投资者和生产者获利。更为有趣的是，投资者和生产者是完全可以自由加入和退出的，即不需要任何烦琐的程序，也不需要任何人的批准。一个人可以随时成为这个公司的投资者、生产者以及消费者等任意一种角色或者全部角色。

比如购买以太币，使用了以太坊上应用的以太坊开发者就扮演了全部的角色。

而这样的区块链企业模式，让如收入、利润等传统的一些概念彻底消失了，在没有收入概念的情况下，依旧能够让投资者和生产者获利，能促使他们的企业变得越来越好，还能促使更多人使用企业的产品或服务。更简单的关系、更高的流动性让他们比传统企业变得更加有活力，也更加高效。

传统的公司模式起源于中世纪的欧洲，所以它肯定不是一个为互联网设计的模式。而今天互联网已经彻底地改变了这个世界的运作模式，也许也会改变公司的运作模式。从运作方式来看，区块链公司才是真正为互联网设计的公司模式。尽管我们还不知道它是否有机会在未来成为主流的企业形式，但是很有可能会有更多的人意识到，这种公司也许有可能会彻底改变现有的商业社会。

第四章 区块链项目介绍

一、区块链项目的基础架构

（一）基础架构

1.以太坊

（1）以太坊的概念

Ethereum是一种新的去中心化账本协议，不是一种竞争币。以太坊的理念基因中不仅含有比特币基因，还含有BitTorrent、Java和Freenet的基因。从产品的角度而言，它是一个通用的全球性区块链，可以管理金融和非金融类型应用的状态。

本质上，以太坊促成去中心化的商业逻辑（business logic）——也被称为智能合约，它是一个包含价值，当特定条件满足会被自动打开的加密“箱子”（boxes）。商业逻辑在区块链云上（不需要服务器）执行，在多方之间自动执行给定协议的条款。它们是“去中心化应用”（DApp）的基本构件。从前端角度而言，以太坊拥有一个强大的专用浏览器，使用户可以方便地安装和使用DApp。

这一新技术将促成Web3.0的基础设施的建立，将会建立在三层部件之上：作为客户端的先进浏览器，共享资源的区块链账本，以及以去中心化方式运行智能商业逻辑程序的计算机虚拟网络。

与比特币相比，以太坊建立了一种新的密码学技术基础框架，在其上开发应用更加容易，同时允许应用共享一个可行的经济环境和可靠安全的区块链。

它具有多种意义。对于开发者来说，写新的应用时，将极大地节约成本和更加高效。对于非技术人员来说，通过分拆中心化的功能，并将它分散到去中心化结构中，提供一个重新想象现有商业，或者创建新机会的可能。以太坊帮助任何希望完全借助区块链开发去中心化应用、编码任意复杂商业逻辑、发布自治代理和管理关系的人。

以太坊是一种特殊的云计算，不仅高效、节省成本，也非常安全可靠。同时，它还拥有一套完整的创建应用的工具。以太坊系统可以用于安全地执行多种服务，包括：投票系统、域名注册、金融交易所、众筹平台、公司管理、自我执行的合约和协议、知识产权、智能财产和分布式自治组织。

以太坊正在全球范围内激发商业和社会创新，为前所未有的应用打开了大门。从长期来看，它所引致的结果将影响经济和控制结构。数以千计的企业家和开发者正在创建和实施基于以太坊的新理念、新项目和创业公司。为了在未来保持竞争力，现有的组织、商业和IT领导者应该探索如何利用以太坊重构现有服务或者在现有服务上进行创新。

（2）以太坊VS比特币

作为起点，可以对以太坊和比特币进行比较，因为比特币似乎已经被理解了，至少被那些希望理解它的人所理解了。

初看起来，比特币和以太坊都是开源平台，具有四项共同点：底层的密码学货币、区块链、去中心化的共识证明机制和维护网络的矿工。这一切使人们容易混淆比特币和以太坊，觉得它们肯定是类似的事物。但是，当你深入探究时，会发现两者的不同点多于相同点。四项共同点

的每一项在以太坊和比特币中的作用和目的都是不一样的，出于这个原因，以太坊会朝着一个不同于比特币的方向发展。

比特币最初被设计成一个用于交易货币价值的去中心化密码学货币网络，比特币区块链的主要目的是：为这些金融交易提供信任支撑。只是到了最近，比特币区块链才开始在非金融应用中被发现使用的情景。因此，比特币区块链的可编程性只是事后的想法，并不是最初就有的设计，虽然侧链的提议希望让编程更加容易。与比特币相反，以太坊从第一天起就被构想为一个去中心化应用软件开发平台，它的区块链被设计为支持去中心化应用的运行。所以，以太坊的设计有幸从比特币的经验中学习，并改进了比特币的缺点。例如，与比特币10分钟的区块确认时间相比，以太坊区块链执行确认的速度更加快速，确认时间在5~30秒范围内。

以太坊的目标是实现大规模的去中心化应用，这需要以太坊成为一个确定的、可审计的和可预测的计算平台。这不同于比特币的本质——计算是以货币为中心的。因此，为了全面理解以太坊，不能盲目地将比特币的挖矿、密码学货币用途和可编程性推及至以太坊。

首先，以太坊的密码学货币（被称为以太币）并不类似于比特币，因为它的主要目的不是用于商品或者服务的支付，也不是“数字黄金”。这是比特币的重要特性，但以太坊志不在此。以太币更像一种“加密燃料”（**crypto-fuel**）形式的激励，支付运行各种智能商业逻辑程序所需的交易费用（关于“燃料货币”相关知识，请参见后面章节）。除了作为网络燃料以外，以太币也将作为一种数字货币在交易所交易，但是它的价值更多地受交易需求量影响，而不是货币投机者。

以太币类似于云计算费用。当你在云中运行一个应用时，基于你的运行时间、占用的存储空间、数据转移和计算速度，你需要向云计算公司支付相应的费用。以太币费用的新颖之处在于你为运行在区块链上的商业逻辑付费。

其次，以太坊区块链被设计为完全可编程，比比特币更具有经济效率。它具有更大的可扩展性，对于用户可以低成本地使用区块链而言，这是非常关键的要求。因为以太坊不只关注于实现金融交易，所以以太坊区块链的目的不同于比特币。从技术上而言，以太坊的区块大小没有上限，它可以动态地调整。另外，以太坊正在继续致力于提高可扩展性（scalability），这将有益于降低整体的交易成本。

一般而言，当我们思考一个区块链的优良特性时，会考虑到以下的特性，这也是以太坊所擅长的：

- 可编程性（Programmability）；
- 可扩展性（Scalability）；
- 可升级性（Upgradability）；
- 交易可管理性（Transactions Manageability）；
- 可见性（Visibility）；
- 可购性（Affordability）；
- 安全性（Security）；
- 速度 / 性能（Speed/Performance）；
- 高可靠性（High Availability）；
- 可延展性（Extensibility）。

再次，尽管工作量证明是以太坊目前所选择的共识机制，但是它打算进化到更加节省能源的共识机制——权益证明。权益证明已经被证明是一种高效和可行的共识方式，运行的成本更低，攻击的成本更高。

最后，以太坊的挖矿可以由常规计算机完成，不需要比特币那样的专门化挖矿设备，因此以太坊挖矿能够让更多的人参与。任何在自己的电脑上运行以太坊挖矿客户端软件的用户都可以成为矿工，就像BitTorrent允许任何用户公开分享自己的文件一样。这是一个好策略，因为它使普通用户用得起以太坊，不需要过度依赖昂贵的挖矿。这也意味着，与比特币不同，以太坊不需要依靠积累挖矿算力来运行。它更加倾向于通过可负担的挖矿与支付所需计算费用之间的平衡来实现自我平衡。

（3）开发语言

以太坊的软件开发语言是其最大特性之一，因为对区块链进行编程是一项首要目标。以太坊具有四种专用语言：Serpent（受Python启发）、Solidity（受JavaScript启发）、Mutan（受Go启发）和LLL（受Lisp启发），都是为面向合约编程而从底层开始设计的语言。

作为以太坊的高级编程语言，Serpent的设计非常类似于Python。它的设计目标为最大可能的简洁和简单，将低级语言的高效优势与编程风格中的易用性相结合。

Solidity是以太坊的首选语言，它内置了Serpent的所有特性，但是语法类似于JavaScript，这降低了学习门槛，易于被掌握和使用，因为JavaScript是Web开发者的常用语言。因此，Solidity充分利用了现有数以百万程序员已掌握JavaScript这一现状。

以太坊区块链的另一关键特征是它的“图灵完备性”，这保证了以太坊可以解决必需的计算问题。更加准确地说，它是“半”图灵完备的，因为通过对计算量设置上限，避免了完全图灵完备语言存在的无法停机问题。

此外，因为以太坊的语言是为区块链专门设计的，他们在交易的可

视化和活动性上不可思议地提供了在实时性上的粒度。这是一个受人欢迎的功能，但对比特币而言实现起来具有一定的挑战。在比特币上，你需要导入区块链数据库，解析所有的交易，并为了抽取出区块链上的活动情报而查询交易。而用以太坊，你可以在活动的区块链上实时发起一个特定的地址要求。

（4）去中心化应用

以太坊支持多种开发语言是非常重要的，因为这使得开发者可以选择自己喜欢的语言，可以更加容易和高效地写去中心化应用。

一个DApp是由智能合约和客户端代码构成的。智能合约就像加密的“箱子”，包含价值，只有当特定条件被满足时，它才能被打开。它封装了一些逻辑、规则、处理步骤或者双方间的协议。当它们被发布在以太坊上时，网络会执行它们的分支（ramification）。

从架构角度而言，DApp非常类似于传统的Web应用，主要区别是：在传统Web应用中，客户端有Javascript代码，由用户在自己的浏览器中执行，服务器端的代码由公司的主机运行；但是在一个DApp中，你的智能逻辑运行在区块链上，客户端代码运行在特殊浏览器——Mist里面。

另外，DApp可以与其他Web应用或者去中心化技术相交互或者连接。例如，一个DApp可以使用去中心化的消息服务（例如Whisper），或者去中心化的文件（例如IPFS）。从Web应用的角度而言，例如谷歌这样的公司可能打算从一个去中心化的信誉服务中获取数据，或者Bloomberg（彭博）的数据来源种子可能打算与一个金融DApp进行交互。

（5）以太坊客户端

以太坊包括一个专用的客户端浏览器，使用户可以运行各种各样的DApp和发布智能合约。这一浏览器（以太坊浏览器被称为Mist）易于使用，所以DApp和智能合约能够被大量用户使用。从降低用户使用门槛角度而言，Mist是一项突破性成就。它的作用等同于浏览器之于互联网，或者iTunes（苹果公司一款数字媒体播放应用程序）之于数字化内容下载。Mist具有特殊的安全层、密钥管理、去中心化账户管理（即用户账户由用户拥有并控制，而不是第三方机构），以及与区块链相关的组件，这一切使Mist成为普通用户运行或者管理区块链去中心化应用不可或缺的工具。普通用户不需要理解技术方面的东西。

从用户体验角度而言，你可以在Mist中使用DApp，就像你通过常规浏览器与网站进行交互一样。例如，一个纯DApp（例如预测市场Augur）就在以太坊Mist浏览器中。然而，这些服务也可以通过一个常规浏览器以更加传统的Web2.0的方式实现。

（6）以太坊虚拟机

当你想到这些自足的逻辑脚本——运行在区块链上，在其上存储数据，向发起人返回一些值时，就像运行在云中的程序。简单地说，这些智能合约就是运行在以太坊虚拟机（EVM）上的代码。因此，这类似于一个去中心化的虚拟计算服务，但是它不存在网站服务器这样的负担，它被设计成点对点网络，所有参与者都可以运行，可以安全地（通过加密和数字签名）向区块链写入数据和代码，读取上面的数据和代码。

以太坊虚拟机概念是非常重要的，因为它是以太坊项目的另一个主要创新。如果你不理解EVM，那你就不理解以太坊。

EVM“位于区块链之上”，但是，实际上它是由许多互相链接的计算机组成的，任何人都可以上传程序，让这些程序自我执行，保证现在和所有以前每个程序的状态总是公共可见的。这些程序运行在区块链上，

严格地按照EVM定义的方式继续执行。这使任何人都可以为所有权、交易格式和状态转换函数创建商业逻辑。

（7）以太坊核心和生态系统

在最底层，以太坊是一个多层的、基于密码学的开源技术协议。它的不同功能模块通过设计进行了全面的整合，作为一个整体，它是一个创建和部署现代化的去中心化应用的综合平台。它被设计为一个通用的去中心化平台，拥有一套完整的，可以扩展其功能的工具。

虽然，以太坊看起来像由多个互相联系的开源项目构成的混合体，但是它的进化一直被明确目标引导着，以此保证各个组件可以协同地组装在一起。

像大多数软件平台一样，以太坊核心的外围是一个由合作者、技术交互扩展（interchange extensions）、应用和辅助服务组成的丰富的生态系统，用于增强以太坊的核心地位。从功能角度而言，我们可以将以太坊生态系统拆分成三块：

第一，核心协议技术，点对点共识、虚拟机、合约、密钥、区块链、软件语言和开发环境、货币（燃料）、技术整合和中间件服务（middleware services）。

第二，应用，客户端软件（Mist或者AlethZero）、挖矿、监控服务（monitoring services）、去中心化应用和其他第三方应用。

第三，辅助服务，主要通过维基、论坛、以太坊学院、网站、赏金激励、未来的开发者会议实现的教育、研究、学习和支持。

在应用方面，截至2016年4月，已经有近200个第三方项目、产品、技术扩展和完全或者部分基于以太坊的成熟商业。这些应用包括：预测市场、去中心化交易所、众筹、物联网、投票和管理、赌博、信誉系

统、社交网络、聊天消息系统、保险、医疗保健、艺术、交通工具共享、分布式自治组织、交易（金融工具或者商品）、会计、社区、电子商务、物理安全、文件存储、所有权登记、内容、小微交易、社区管理、云计算、汇款、智能合约管理、智能资产、钱包、食品、制造业、数据存储、供应链等。

所有这些生态系统的组成部分促成了以太坊进入金融和非金融领域。以太坊的可编程特性提供了超越比特币脚本语言更加强大的功能，因为它具有图灵完备性、价值知晓（value-awareness）、区块链知晓（blockchain-awareness）和状态转换逻辑能力。

（8）以太坊主要的进展

2013年11月：当时在加拿大的18岁俄罗斯少年、科技奇才维塔利克·比特林（Vitalik Buterin）创建了初始的以太坊概念和基本代码，以太坊的核心理念开始有了一个明确的提法。

2013年12月：维塔利克·比特林发布了原始概念白皮书。

2014年9月：以太坊为期42天的以太币预售结束，一共筹集到31529.36369551个比特币，一共售出60102216个以太币，价值约1800万美元。

2014年11月：维塔利克·比特林击败Facebook（脸书）创始人马克·扎克伯格（Mark Zuckerberg），获得2014年IT软件类世界技术奖。这个奖项表彰了维塔利克·比特林设计发展比特币2.0平台以太坊的突出成就。

2015年7月31日：历经18个月的等待，终于迎来了其Frontier版本平台的正式推出，Frontier阶段只有命令行客户端，下一阶段将推出易用的客户端Mist和AlethZero。

2015年9月30日：维塔利克·比特林宣布，以太坊得到了中国跨国巨头万向集团的资金支持，该集团已推出了一个非营利性的区块链实验室（Blockchain Labs）。万向集团代表方证实了这一消息，区块链实验室最近购买了50万美元的以太币，作为支持该技术的部分尝试。

2016年1月21日：全球最大的区块链联盟R3 CEV已发布了首个分布式总账实验，其使用了以太坊和微软Azure的区块链即服务（BaaS），并涉及其11家成员银行。这个由R3管理的私有点对点分布式总账，连接了巴克莱银行、BMO（蒙特利尔）银行金融集团、瑞士信贷银行、澳大利亚联邦银行、汇丰银行、法国外贸银行（Natixis）、苏格兰皇家银行、道明银行、瑞士联合银行、意大利联合信贷银行以及富国银行。

2016年3月12日：以太坊发展达到新的里程碑。格林尼治时间上午3时15分，该项目总市值达到10亿美元。Homestead进入测试阶段的声明之后，以太坊市值开始了爆炸式增长。单日活动节点增加22%，之后一直呈平稳增长态势。以太币持续一个月成为交易量第二大数字货币。这个新的里程碑明显拉近了以太坊与比特币的差距。后者最高市值为63亿美元。

2016年3月15日：发布了Homestead，公司第一款软件应用。上一个版本Frontier的唯一特征是命令行界面，Homestead会对用户平台搭建功能进行扩展，提供建立概念证明机制的便利以及保证最少可用产品数量。

（二）Hyperledger

2015年底，IBM宣布参加由Linux基金会领头的开源区块链项目开放式账本项目（Open Ledger Project），后来更名为超级账本（Hyperledger）项目。该项目一经公布便受到了金融、科技行业和区块

链行业的广泛关注，除了IBM以外，该项目的参与者来自在金融科技行业和银行业颇具影响力的企业如英特尔、思科、伦敦证券交易集团、摩根大通、富国银行、道富银行。

至2016年2月，该项目的参与者已经增加到了30家，包括荷兰银行、纽约梅隆银行、芝加哥交易所集团、ConsenSys、NTT数据、Red hat、Symbiont等。在2016年4月，又有10个新公司加入该项目并注资，这10家新公司分别是Blockstream、Bloq、eVue Digital Labs、Gem、itBit、Milligan Partners、Montran Labs、Ribbit.me、Tequa Creek Holdings和Thomson Reuters。

Linux基金会是全球顶级开发人员和公司首选，通过组建一个生态系统，能够加速推动技术开发和商业吸取。与全球开源社区一起，通过创建投资历史上最大的共享技术，解决了最难的技术问题。成立于2000年的，Linux基金会今天提供了工具、交易和所有开源项目，没有任何一家公司能够达到这样的经济影响力。Linux基金会（Linux Foundation）和Linux标准库（Linux Standard Base）都是Linux基金会的商标。Linux是Linus Torvalds的商标。

自成立以来，超级账本项目已经收到来自多个企业的代码和技术，其中包括Blockstream、Digital Asset、IBM和Ripple。其他社区成员也在考虑如何贡献他们自己的力量。就如同其他的开源项目一样，欢迎来自任何时间、任何人的技术贡献，并将会由新组成的技术指导委员会（Technical Steering Committee, TSC）进行审核，该委员会是由行业中领先的技术专家组成的。TSC致力于开放和透明的讨论、流程和决策。这个小组将负责该项目的技术方向，工作小组会管理多个代码库的各种贡献。TSC将会评估贡献提议，并且通过一个开放社区流程，来打造出最初和统一的代码库。

由数字资产控股捐献的商标“超级账本”，把它送给Linux基金会。该商标将会完全交给超级账本项目理事会进行管理，并且需要Linux基

金会的审批。

超级账本项目公开宣布了它的治理结构。董事会将会指导企业决策、市场营销，确保技术社区和成员之间的一致性，目前TSC成员进行公开提名。

超级账本项目是让成员共同合作，专注于开放的平台，将会满足来自多个不同行业各种用户案例，以简化业务流程。由于点对点网络的特性，分布式总账技术是完全共享、透明和去中心化的，因此非常适合在金融，以及制造、银行、保险、物联网等无数个其他行业的应用。通过创建分布式总账的公开标准，实现虚拟和数字形式的价值交换，例如资产合约、能源交易、结婚证书、能够安全和高效低成本地进行追踪和交易。

Linux基金会执行董事吉米·策姆林（Jim Zemlin）表示，超级账本项目已经以惊人的速度在进行，证明了有许多压抑的兴趣和潜力正期待被释放，现在全球企业需要一个分布式总账技术的跨行业开放标准。

（三）R3 CEV

1.R3的成立

创立于2015年9月的R3公司专门负责合成银行业区块链技术开发的行业标准以及用例，致力于为银行提供探索区块链技术的渠道以及建立区块链概念性产品。首席执行官戴维·鲁特（David Rutter）表示，长久以来R3公司一直坚信，分布式总账技术可能会像互联网改变媒体和娱乐业那样改变金融服务业。该联盟成立之后，召开了一系列的研讨会。尽管有关该项目的细节还很稀少，但项目代表都表示R3希望建立称为“全球金融结构”的东西，或者说是针对银行业需求的区块链和分布式分类

账，并且精心制作它的输入。

戴维·鲁特在行业内有着广泛的人脉网络和在华尔街顶级机构超过30年的领导经验，以及对市场的深度了解，这使他有独特的方式接触和洞察到R3的客户。他早期全球最大的交易经纪商ICAP（Internet Content Adaptation Protocol），担任电子经纪首席执行官，并且还领导BrokderTeck固定收入和EBS（紧急燃油附加费）外汇平台，这是全球两个最大的电子场外交易平台。

尽管开始R3区块链被设计为一个开源形式，但是尚未决定最后的开放形式。目前也没有确定是否会被限制在成员银行中。这将会影响“节点”应该如何来确认每一笔交易的方式。成员银行非常有兴趣参与区块链技术所提供的广泛应用测试，包括金融交易、处理银团贷款，对场外衍生品和市场借贷进行清算。一个在伦敦的开发团队目前正在编写一个开源、通用的“共享账本”，将会让银行大幅度降低协调成本。

2.45个联盟成员

R3公司在2015年12月17日宣布，银行“梦之队”已经完成首轮团队招募。R3区块链联盟迎来了当年最后12个新成员，分别是桑坦德银行、丹麦丹斯克银行、意大利圣保罗银行、法国外贸银行、野村证券、北方信托、OP金融集团、加拿大丰业银行、三井住友银行、美国合众银行、西太平洋银行和BMO金融集团。此外，据称这些银行还将投资R3公司。

于是R3区块链联盟的成员从最初的9家银行，扩大到目前的42家银行。R3表示，其允许银行加入的“初始窗口”已经关闭，该联盟将在2016年寻求与非银行金融机构和团体合作，扩大要整合的产业范围。

尽管R3在2015年底曾表示，截至2015年12月就已经停止吸纳更多会员，可是在2016年3月的采访中，R3总经理查理·库珀（Charley

Cooper) 宣布第二轮合作已经开始了, 并且日本SBI (Strategic Business Innovator) 控股株式会社是第二轮合作第一个加入的企业。

日本SBI控股株式会社, 即SBI集团, 原软银投资 (Soft Bank Investment), 成立于1999年, 已发展为以投资和互联网为平台在全球展开业务的大型综合金融集团。截至2013年9月末, SBI集团在全球拥有180家子公司 (包括中国5家), 其中6家在中国香港、日本、韩国上市, 业务遍及北美、欧洲、南美、中东及东南亚各国。截至2013年9月, 集团总资产达2.85万亿日元, 资产管理规模为4800亿日元。

在2016年4月, 韩国金融机构韩亚金融集团 (Hana Financial Group) 和巴西银行伊塔乌先后加入了R3区块链联盟, 使得R3联盟的成员扩充到45个。

2016年5月下旬, 中国金融巨头中国平安宣布加入R3 CEV区块链联盟, 有效地开启了世界第二大经济体的大门。中国平安市值高达900亿美元, 有27家子公司, 业务涉及很多行业, 包括寿险、银行和证券。

据称2016年初, 中国平安首席创新官丹尼尔·图 (Daniel Tu) 致电R3 CEV全球执行董事克莱夫·库克 (Clive Cooke), 表示希望加入R3。在克莱夫·库克与中国平安CEO (首席执行官) 马明哲初次会谈之后说, 中国平安在中国有很大的网络, 是完整独立的生态, 是R3进入中国的最好契机, 而且中国平安对待区块链技术的态度很积极、实际, 相信中国平安对区块链的认识和开发以及与R3 CEV的合作会极大推进区块链在中国的发展。丹尼尔·图和中国平安区块链倡议的主管杰西卡·唐 (Jessica Tang) 成立了包含中国平安技术部和金融部的15个员工小组, 还有集团子公司的首席技术官。尽管还不知道中国平安内部区块链小组的工作内容, 但是有消息指出, 中国平安在开发两个概念证明机制, 公司内部在努力地学习区块链技术。

在6月, 香港人寿保险公司AIA和丰田金融 (Toyota Financial

Services）分别宣布加入到R3联盟中，其中丰田金融表示希望把分布式账本技术应用于汽车供应链和互联网汽车系统。

截至2016年6月，R3 CEV的成员伙伴已经达到约50家，并且越来越多的亚洲大型机构加入其中，其影响力正在从欧美扩张到全球更多地区。

表4.1 R3 CEV区块链联盟主要成员

序号	英文名	中文名
1	Banco Bilbao VizcayaArgentaria	西班牙对外银行
2	Banco Santander	桑坦德银行
3	Bank of America	美国银行
4	Barclays Bank	巴克莱银行
5	BMO Financial Group	蒙特利尔银行金融集团
6	BNP Paribas	法国巴黎银行
7	BNY Mellon	美国纽约银行梅隆公司
8	Canadian Imperial Bank of Commerce	加拿大帝国商业银行
9	Citigroup	花旗银行
10	Commerzbank	德国商业银行
11	Commonwealth Bank of Australia	澳大利亚联邦银行
12	Credit Suisse	瑞士信贷银行
13	Danske Bank	丹麦丹斯克银行
14	Deutsche Bank	德意志银行
15	Goldman Sachs	高盛集团
16	Hana Financial Group	韩亚金融集团
17	Hongkong and Shanghai Banking Corporation	汇丰银行
18	Internationale Nederlanden Group	荷兰国际集团
19	Intesa Sanpaolo	意大利联合圣保罗银行
20	ItaúUnibanco Holding	伊塔乌联合银行控股公司

21	JPMorgan Chase	摩根大通
22	Macquarie Group	麦格理集团
23	Mitsubishi UFJ Financial Group	三菱日联金融集团
24	AIA Life Insurance Hong Kong	香港人寿保险公司 AIA
25	Mizuho Bank	日本瑞穗实业银行

序号	英文名	中文名
26	Morgan Stanley	摩根士丹利
27	National Australia Bank	澳大利亚国民银行
28	Natixis Bank	法国外贸银行
29	Nomura Securities	野村证券
30	Nordea Bank	瑞典北欧联合银行
31	Northern Trust Bank	美国北方信托
32	OP Financial Group	OP 金融集团
33	Royal Bank of Canada	加拿大皇家银行
34	Royal Bank of Scotland	苏格兰皇家银行
35	Scotiabank	加拿大丰业银行
36	Strategic Business Innovator	日本 SBI 控股株式会社
37	Skandinaviska Enskilda Banken	瑞典北欧斯安银行
38	Societe Generale	法国兴业银行
39	State Street	美国道富银行
40	Sumitomo Mitsui Banking Corporation	三井住友银行
41	Toronto-Dominion Bank	多伦多道明银行
42	UniCreditSpA	意大利联合信贷银行
43	Union Bank of Switzerland	瑞士银行
44	US Bancorp	美国合众银行
45	Wells Fargo	美国富国银行
46	Westpac Banking Corporation	西太平洋银行
47	Ping An Insurance (Group)	中国平安
48	Toyota Financial Services	丰田金融

3.五种技术路线和八个概念证明

在2016年3月，R3 CEV宣布正在研究五种区块链技术路线来提供金融服务，其中以太坊位居列表榜首。以太坊项目的创始人比特林表示，使用以太坊正在积极研发的“代码库”，无论是私营区块链企业还是财团均“拍手称赞”。

以分布式总账平台以及专业应对成熟金融玩家的能力而闻名的Chain也是整个项目中颇有价值的一分子。其他参与者还包括Eris Industries、IBM（通过自身区块链服务部门）以及英特尔的新科技集团。所有参与方均同意R3 CEV的前行方式与通过展示而非主张的加速运用区块链技术的途径。

R3 CEV的一位高管在2016年4月的区块链和分布式总账大会（Blockchain & Distributed Ledger Conference）上表示，目前R3 CEV正在以探索分布式总账简化华尔街众多交易以及方便监管的途径，测试至少八个概念证明，分别是互操作性、支付、结算、金融交易、企业债券、回购、掉期和保险。

（四）Corda

到了2016年4月，R3 CEV宣布了它们首个分布式总账应用Corda，而非使用大家都认为的类似于比特币的区块链技术。R3宣称Corda与比特币的非许可型交易分布式总账截然不同，是为金融机构量身定制的应用。这个应用唯一去中心化的信息由银行会员决定。在R3的博客文章中，该项目负责人兼集团首席技术官理查德·布朗（Richard Gendal Brown）指出了Corda与大多数人眼中的区块链的关键区别。

理查德·布朗是联盟在2015年9月从IBM挑选的项目领导人，他在文章中这样描述Corda：我们需要简化业务逻辑编写并与现存代码兼容。我们需要注意系统可互操作性，并在企业建立协议时，提供企业间协作

流程支持。

不同于在系统节点间保存完整交易历史的比特币区块链，布朗强调Corda只会传播经过认证的交易记录。Corda会给监管机构提供“监管观察员节点”，可以从这个节点监控系统运作。包括Overstock的t0平台也在区块链系统中搭建这个功能。R3联盟会在随后几周内进行Corda测试，并且在未来几个月内公司还计划发布“作为公司诸多项目之一”的开源平台核心内容。

布朗说，Corda的名字来源有两个：该名字前半部分听起来像“accord”（协议），后半部分来自“chord”（弦，圆上两点间最短的直线）的定义。这个圆就代表R3网络中的银行。

Corda的主要特点包括：

- 没有多余的全球数据共享，只有有合法需求的参与方可以按照协议获取数据；
- Corda编写和配置在企业间流转，无中心控制者；
- Corda在企业间单个交易水平达成共识，而不是在系统水平上；
- 系统设计直接支持监管观察员节点；
- 交易直接由交易双方验证，而不是由一大群不相干的验证者进行；
- 支持多种共识机制；
- 记录了智能合约代码和人类语言法律文件的清晰联系；
- 用行业标准工具创建；

·没有原始数字货币。

代码完善之后，Corda会采取开源形式。

关于区块链提供的服务，布朗的理解为，比特币、以太坊等其他变化版本底层的区块链技术服务包括五个主要方面，即共识、有效性、唯一性、不可更改性和认证。

区块链最重要的特性是共识。关于比特币，大家共同的认知是比特币有哪些没被消费的收益以及消费比特币需要的条件。这些认知是所有全节点用户共有的。

有效性是与共识有关的特性，帮助人们了解更新建议是否合法，有效性定义了规则方向。

唯一性服务帮助用户了解特定情况下，哪些共享信息更新是有效的。区块链的“反双重支付”特性就提供了这个服务。

不可更改性意味着，一旦某个数据提交了就不能更改了。这个特性可能有点误导性，因为数据实际上是可以更改的。其真正含义是，一旦提交数据，任何人都不能通过篡改其他权益人已经认可的数据来重新进行交易。区块链的做法是：使交易遵循历史交易结果，区块遵循区块链原始信息内容。

认证是最后一个特性，一个私钥对应一个系统行为，这与传统企业系统的“超级用户”账户不同。

分布式总账的新功能是平台的出现，参与网络的怀疑者们共享这个平台，使他们达成共有信息的共识。

金融业定义由共同针对某问题的企业协议确定，合约方在各自系统中记录合约内容。当不同系统最终决定信任不同信息，这时对信息修改

的需要会产生高额费用。两个系统通过信息交换进行交流，很多资源被用于合约方和解，来确保合约方得出相同的结论。

系统记录和管理企业间金融协议就是Corda需要解决的问题，因为这些协议是用行业标准工具建立的并受到必要的监管。该系统关注可互操作性和增量部署，不对第三方泄露机密信息。公司可以查看与对方达成的协议，并确保双方看到的信息一致并向监管机构报备。

（五）Digital Asset Holdings

数字资产控股（Digital Asset Holdings, DAH）是由掉期交易所trueEX创始人兼CEO苏尼尔·希拉尼（Sunil Hirani）和自营交易公司DRW Trading创始人兼CEO道·威尔森（Don Wilson）共同创立的。其目标是成为金融资产交易场所，方便投资者以更低的价格成本和时间成本将传统货币和数字资产进行转换。

前摩根大通高管，全球大宗商品交易界“一姐”，外号是“金融女皇”的布莱斯·马斯特斯（Blythe Masters）在2015年3月加入了DAH，正带领团队开发一种基于区块链系统的证券和资金转移系统。

没有什么比“CDS（信用违约掉期）女皇”转投区块链技术更有说服力了。伦敦《卫报》称她是“发明了大规模杀伤性金融武器的女人”，而《新闻周刊》的说法是这些武器“放出了恶魔”，摧毁了金融系统，引发了2008年全球金融危机。最终的结果是银行在其资产负债表中隐藏了高达55兆亿美元的有毒资产。布莱斯·马斯特斯过去被人们称为“CDS之母”，在经济危机后被称为“世界摧毁者”。2014年，摩根大通的大宗商品业务超越所有竞争者，成为华尔街的头把交椅。但就在这一年，摩根大通迫于监管压力以35亿美元将该部门出售。马斯特斯随后也宣布辞职。

离开摩根大通之后，马斯特斯略微沉寂了一段时间，之后便加入了DAH，重新回到了公众的视野之中。2015年12月，区块链初创公司又在团队中添加了两名在金融服务方面经验丰富的人，吸收了来自软件制造商SunGard和国际支付网络SWIFT的人才。前SunGard总裁兼首席执行官克里斯托博坎德·康德（Cristóbal Conde）将出任执行董事。SunGard创建于1982年，最近被富达国民信息服务公司（FIS）以51亿美元的价格收购。而担任美洲首席执行官及SWIFT证券部门负责人的克里斯·丘奇（Chris Church）将成为Digital Asset公司的首席业务发展官。对于这两位负责人的加入，马斯特斯表示，克里斯托博坎德和克里斯在金融和科技领域有着超过50年的丰富经验，他们不仅对市场有深刻的认识，而且对Digital Asset正在构建的东西有独到的见解，他们的存在对公司不断发展业务的价值是无法衡量的，马斯特斯还表示在该初创公司的收购稳定下来之后，领导团队会继续扩建。

作为曾经的摩根大通商品业务主管，马斯特斯是使用信贷衍生品的先驱，她在摩根大通的成功就来自20世纪90年代她对这些产品将彻底改变银行业的认识。而如今的马斯特斯依然和以往一样高调。她不仅警告美国可能在区块链竞争中落后，而且信誓旦旦地告诉银行业，区块链将变革一切。她说银行目前正在面对一个“收入越加困难的环境中”，并且打算通过裁员来降低成本。但是她认为，这不是一个可以持续的方式。

她指出，区块链技术有足够的潜力来降低成本和风险，它能够帮助自动化来执行那些目前还是由人工来操作的，在后台运行的复杂任务系统，并且有助于降低错误风险。人们应该严肃对待这个技术，它就像20世纪90年代初的互联网，意味着财富在向你招手。华尔街最终将会接受比特币底层的区块链技术，即使这可能还需要5~10年的时间。

2015年10月20日，在曼哈顿举办的《经济学人》梧桐树会议上，她这样说道：“对于银行而言，它们有拥抱新技术的动力.....那就是恐惧和贪婪的结合。”这句话被许多人认为是银行业对区块链态度最好的描

述。

（六）ChinaLedger

2016年4月19日，由中证机构间报价系统股份有限公司等11家机构共同发起的区块链联盟——中国分布式总账基础协议联盟（China Ledger联盟）宣告成立，上海证券交易所前工程师白硕出任了该联盟技术委员会主任，联盟秘书处则设在了万向集团旗下的万向区块链实验室。

白硕在发布会上表示，中国不能在还没有想清楚区块链在中国金融领域如何落地的情况下，贸然与国际上的区块链组织接轨，也不能让每个金融机构各自为战成为一盘散沙，而需要凝聚中国共识，开垦中国的区块链试验田。

该联盟将致力于开发研究分布式总账系统及其衍生技术，其基础代码将用于开源共享。主要有4个目标：

- （1）聚焦区块链资产端应用，兼顾资金端探索；
- （2）构建满足共性需求的基础分布式总账；
- （3）精选落地场景，开发针对性解决方案；
- （4）基础代码开源，解决方案在成员间共享。

目前联盟首批11家成员包括国企和民企，分别为中证机构间报价系统股份有限公司、中钞信用卡产业发展有限公司北京智能卡技术研究院、浙江股权交易中心、深圳招银前海金融资产交易中心、厦门国际金融资产交易中心、大连飞创信息技术有限公司、通联支付网络服务股份

有限公司、上海矩真金融信息服务有限公司、深圳瀚德创客金融投资有限公司、乐视金融、万向区块链实验室。

其中，中证机构间报价系统股份有限公司原名中证资本市场发展监测中心有限责任公司，是经中国证监会批准并由中国证券业协会按照市场化原则管理的金融机构。

据万向区块链实验室透露，联盟成立之后，11家单位将各自派出区块链的研究人员，共同开发中国的底层分布式总账系统。成立China Ledger联盟，期望能够开发出符合中国政策法规、国家标准、业务逻辑和使用习惯的底层区块链基础设施。

万向区块链实验室是由中国万向控股出资成立的非营利性的专注于区块链技术的前沿研究机构。发起人为中国万向控股有限公司副董事长兼执行董事肖风博士、以太坊创始人比特林、BitShares创始人沈波。实验室将聚集领域内的专家就技术研发、商业应用、产业战略等方面进行研究探讨，为创业者提供指引，为行业发展和政策制定提供参考，促进区块链技术服务于社会经济的进一步发展。中国万向控股也承诺每年向区块链实验室捐赠100万美元，以资助相关产业研究及发展。

二、支付汇款

（一）Circle

杰里米·阿莱尔（Jeremy Allaire）在2013年10月创立了Circle，旨在使比特币“简单易操作，类似Gmail（谷歌邮箱）、Skype（微软的网络电话）和其他客户服务”，该公司迅速获得大量融资。在2014年中旬从Breyer Capital、Accel Partners、General Catalyst Partners和Pantera Capital等投资商那获得2700万美元，成为数字货币领域资金最为充足的公司之一。而这批风投家又选择在2015年重聚，进行另一轮融资。由高盛投资公司和总部位于中国的IDG Capital Partners共同主导，为Circle带来了5000万美元的资金，其总投资额达7700万美元，Circle总市值一跃升至2亿美元。

高盛策略性投资小组的负责人汤姆·杰索普（Tom Jessop）表示，Circle在全球支付业务中有着巨大的发展潜力。因为随着金融业务行业不断数字化和开放化，高盛在其中看到了许多发展的机会和可借鉴的思路，将全球市场通过技术创新来推动。高盛认为，Circle的产品视野和非凡的管理团队在众多数字支付服务中脱颖而出，这点非常有吸引力。

预期Circle利用比特币区块链的超低息交易后，可以在世界范围内提供即时免费的资金转账。就这点而言，该公司的负责人很好地将其发展图景展示给了华尔街和海外的投资人。IDG Capital Partners之前被中国公司百度和小米成功融资过，目前也准备帮Circle在亚洲开设分行。消费金融目前正处在一个深刻的转型期，移动支付应用持续发展，非传统金融产品不断涌现，IDG预感Circle能够准确抓住并跟上所有这些趋势和潮流。

除了融资5000万美元，Circle还宣布推出新功能，允许用户只使用美元进行交易。用户将来或可持有、转出并即时接收美元，不需要额外收费，同时还受到联邦存款保险公司和美元稳定价值的保护。这使Circle从一个简单的比特币公司变身为类似贝宝和传统银行的机构。

Circle希望利用比特币作为免费的互联网支付网络，使各国法定货币在全球范围内毫无阻碍地顺畅流转。通过与像IDG这样的海外公司合作，Circle可以向使用各国法定货币的用户提供金融服务，比如人民币和日元。

尽管中国方面对支付系统的监管结构比较复杂，但这些国外合作还是取得了一些进展。目前，Circle作为年轻的新兴公司，专注于为美元功能开发。使用美国账户储备、发送和接收美元的功能已推出，并且在未来将会不断完善。

该发展会进一步模糊法定货币和数字货币之间的界限，但同时保有两种系统的最优特质。选择美元作为融资单位的用户可以受联邦储蓄保险公司投保的硅谷银行保护，不用承担数字货币价值急剧变化所导致的损失。同时，美元持有人可以轻松地向任何比特币接收人完成支付，并且这些操作不需要用户对比特币非常了解，也不受价格变化的影响。Circle相信，比特币会成为一种全球适用的支付网络，而不是一种保值手段。

像Circle这样有创新力的公司还在继续使用比特币区块链作为全球金融系统，而其中的发展潜力也受到许多主要机构投资者的关注。Circle除了在现有的比特币基础业务外提供法定货币的储备和支付，更逐步对货币本身进行着独家定义。

（二） Abra

当今世界，跨国银行之间的转账需要两三天时间，甚至像Venmo这样表面上看似即时的支付应用，实则也并非如此。而比特币的技术可以让汇款瞬时、安全地在个人端之间完成。Abra就是这样一家解决汇款问题的初创企业，宣布其应用将很快提供给所有在美国和菲律宾的注册用户，商家也可以使用Abra提供的服务接受消费者的电子现金。Abra公司宣布于2015年9月的A轮1200万美元融资，已新增加了来自美国运通及拉丹·塔塔（Ratan Tata），印度塔塔集团名誉主席，掌控96家公司的印度资本巨鳄的战略投资。而美国运通的参与，也标志着投资区块链创业公司的传统金融巨头机构，又新增了一家，而在此前，已投资的机构还包括纳斯达克、Visa、高盛以及纽约证券交易所。

美国运通风投管理合伙人哈舒尔·桑吉（Harshul Sanghi）表示，由于人们和企业的交易变得更加全球化，就需要有更为方便、经济的方式来转移资金，因此区块链可以在汇款和商业的发展过程中发挥重要的角色，尤其是在新兴市场。

Abra的新商家服务功能，可以让任何商家为其Web或手机APP添加Abra商家API，以接受来自客户的支付（只输入手机号进行结账付款）。在这里，支付的功能与现金是完全相同的。但在发生欺诈的情况下，将不会有信用卡支付所提供的欺诈保护，受害者需要直接与商家进行协商。

该应用程序可允许用户在他们的手机上存储数字形式的货币，通过Abra出纳员采取网络或传统银行路由的方式，将这些钱发送至世界各地任一手机号上，并将这些数字现金兑换成现金。因为所有的钱都是直接存储在手机上的（法币，不是比特币），而Abra承诺永不接触这些钱。比如，用户A想要给朋友发送5美元，那么他所需要的就是对方的手机号。在后端，Abra创建了一个索引，会将这些电话号码映射到比特币区块链上的公共地址。如果收钱方在手机上并没有安装Abra，那么他就会收到一条提醒他进行安装的短信。在交易的幕后，比特币区块链记录了

发钱方汇款5美元给收钱方的整个过程，完成汇款后，双方的应用程序就会显示账户的余额变化（该应用程序还需考虑到数字货币对法币的兑换问题，以便汇款值不会受到比特币的价格波动影响）。如果收钱方希望把这一数字现金转换为纸币现金，Abra会和出纳员网络工作，包括充当ATM机（自动取款机）的个人，还有大型的零售商，都可以扮演网络的出纳员。

像美国这样的国家，消费者们会更倾向于银行来进行取现。然而，在发展中国家，许多个人和小型便利店则更可能成为出纳员。出纳员可以设置自己的收费标准，而Abra则会对每笔交易收取额外0.25%的手续费。

据说Abra已经在2016年上半年完成了A2轮的融资，有一些来自中国的大型IT和金融企业参与了该轮融资。

（三）Align Commerce

Align Commerce公司由前西联汇款总经理马尔万·福兹雷（Marwan Forzley）一手创立，该公司正在寻求颠覆小型企业（SMB）的跨境支付市场。在加盟西联汇款之前，福兹雷还是支付创业公司eBillme的创始人，后来西联汇款收购了这家创业公司，福兹雷也因此加入了西联。

Align Commerce表示，相信跨境支付格局将被打破，而采用新的技术可以帮助减少一些摩擦，这就是使用区块链的原因。其公司产品改进了传统电汇的跨境交易，可以让中小企业发送美元，而接收者收到的则是欧元。最终用户所使用的，仍然是传统的银行账户，然而在支付的中间过程，Align将发送者的资金转换成比特币，然后将这些数字货币在一家交易所卖出，再为接收者换成他们所期望的货币。这种解决方案带来的不仅是成本上的降低，还有其他方面的益处。

Align Commerce有很多的交易所合作伙伴，因此，比特币价格的波动性对该公司的影响并不是很大。此外，区块链可以允许Align为商家客户提供其他好处，比如提供他们汇款的即时信息。在过去，客户可以在网上追查货物，但无法跟踪你的在线支付过程。区块链拥有一个公开透明的跟踪机制，可以帮助客户了解支付的踪迹。他们认为这种新技术与现有的支付方案相比，更经济、更快，也更易于追踪。



图4.1 Align Commerce发起付款的三步骤

由此可见，Align Commerce使用区块链技术，是要取代代理银行在跨境支付过程中进行的工作，该公司认为，这种技术可以为商家客户提供更为经济的交易。看上去其市场定位有点类似于分布式支付协议提供商Ripple，但Align Commerce解释说，这两家创业公司之间并没有争用相同的客户群体，尽管他们在技术方法上有着很大的相似性。首先，Ripple的目标是银行，而他们瞄准的则是小企业市场。其次，Align Commerce当前所使用的是比特币区块链。但公司也表示，如果有需要的话，公司的产品也可以使用Ripple的分布式总账。Align Commerce开

发的是一个应用层，可以切换到任何的数字货币。

为了能够在其管辖区内提供服务，Align Commerce必须要做的一点是，能将比特币兑换成当地的货币，这也就意味着，它会受益于当地比特币交易所的可用性。福兹雷拒绝说出任何具体的合作伙伴，但他表示，在没有交易所覆盖的地区，银行会负责维护相关的交易。公司表示会花更多的时间和精力去扩展交易所，因为这是市场所需要的一个重要发展。

在2015年11月，该公司完成了A轮融资，融资金额达到1250万美元，领投方为硅谷传奇投资公司KPCB，跟投方包括Digital Currency Group、FS Venture Capital、Pantera Capital、Recruit Ventures Partners以及硅谷银行的投资部门SVB Ventures。

此前该公司还于2015年4月获得了一笔种子资金，但并未公布具体的金额，而最新获得的A轮融资，将用于扩展Align公司的服务范围。而作为交易的一部分，凯鹏华盈的一般合伙人兰迪·科米萨（Randy Komisar）将加入该公司的董事会。

（四）Streami

2015年12月25日，韩国区块链汇款创业公司Streami完成了200万美元的种子轮融资。尽管该创业公司是汇款市场的新来者，但其支持方包括韩国最大的金融服务机构之一——新韩银行，该机构投资了大约42.7万美元。此外，Streami还得到了新韩数据系统（新韩银行实体IT公司）的支持，其他投资方还包括支付公司ICB，风险投资公司Bluepoint Partners，以及一群天使投资人。

该公司针对的汇款市场，包括韩国、中国、菲律宾、中国香港、印度尼西亚、新加坡、泰国，旨在帮助这些地区的人们绕过非法货币转移

服务。Streami公司首席执行官李俊恒（Jun Haeng Lee）声称，截至目前，Streami的主要竞争对手是传统的汇款服务提供商以及占据韩国对外汇款市场显著份额的非法金钱转移商。Streami将为加密网络带来可信赖的、规范的流动性，Streami的这轮资金将用于公司在首尔以外城市开设分支机构，并招募新的人才。

ICB公司首席执行官李韩勇（Han Yong Lee）表示，他的公司参与了这一轮融资，希望能够提供更好的以区块链为基础的外汇Fintech服务，并与Streami公司进行合作，以便进一步探索这项技术。

三、数字货币交易所

Coinbase公司成立于2012年6月，业务主要包括比特币钱包和交易平台，让商家和消费者可以用新的数字货币比特币进行交易。它的总部设在加利福尼亚州旧金山市，致力于让消费者更方便地使用比特币，目标是成为比特币界的Gmail。这家公司的CEO布莱恩·阿姆斯特朗（Brian Armstrong）正在领导团队负责让比特币成为一种主流货币。

在美用户可以使用信用卡在Coinbase购买比特币。他们可以轻松地把比特币存在任一在线钱包应用里，并且可以通过电子邮件互相发送比特币，而不需要担心二维码或者那串看似乱码的比特币地址带来的麻烦。他们甚至可以通过短信来控制自己的比特币。

它是如何做到的呢？核心开发者杰夫·戈查克（Jeff Garzik）曾经说过，尽管比特币货币的基础协议已经被开发出来了，但是来充分利用这种货币的第二层服务仍然被需要。这些服务，比如说更加直觉化的支付系统、信用服务、股票交易所以及智能资产，将使得比特币在那些对比特币公钥等概念不感兴趣的主流用户中获得更多的关注。

Coinbase并没有在建设上述服务中的大部分，但它聚焦在使这些服务尽可能地简单易用。Coinbase想让比特币变得更简单，并且如果可以通过使用底层的比特币科技来实现，那么，Coinbase就将先用底层科技来实现，但如果客户要求一些像定期结算，或者订阅支付，或者免费的超小额支付的服务，并且无法想出一条使用底层协议来实现功能的途径，那么，Coinbase将在协议的顶端提供它。当Coinbase的用户在Coinbase钱包间互相发送比特币，他们是把比特币发送到电子邮件地址，而不是比特币地址。这是这家公司提供的众多易用特性之一。

Coinbase的服务可以分解成三大块：用户钱包、比特币买入以及卖

出、商户工具。在这三个领域，它都有竞争对手（比如说BitPay就是它在商户工具领域的对手），但它同样分别拥有不同的优势。例如，它是为数不多的（如果不是唯一的话）提供一个去中心化的比特币生态系统的公司；又如，它提供了钱包的链外（off-chain）交易，以及推荐其他客户的比特币奖励。在商户这边，它使商户可以通过早些时候发布的商户工具来收集寄送地址和电子邮件地址，并且已经开始提供定期支付的功能了，商户们还可以零费率接受微支付。

阿姆斯特朗总是将Coinbase的服务比喻成Gmail，而把比特币比喻成SMTP。SMTP是一个开放的提供基础功能的电子邮件标准，但人们使用Gmail可以做到更多非标准的事情，比如说把日历活动的邀请自动放入Google日历中，又如可以充分利用自动信息优先化处理或者直接在客户端里面以会话的形式查看邮件。Coinbase进行的交易有75%~80%是在内部被处理的，但在需要更多的处理能力的时候，它与合作伙伴Coinbase和Tradehill、bitstamp有合作协议。

从一个一切皆无定数到像比特币这样去中心化的世界里，拥有你自己的生态系统等于拥有一笔宝贵的财富，但公司仍然面临着一些挑战，有一些监管上的不确定因素。公司正在美国范围内进行比特币与法币的兑换，并且它的确已经采取措施以获得在联邦级别上有一张MSB的许可证。然而，在美国不同的州会有不一样的情况。每个州都有自己的监管方法（有的州似乎完全没有），也已经搞定了它自己的“AML”（反洗钱）和“KYC”（了解你的客户）的流程，也在尽最大的努力确保有监管者来问话时，公司可以让他们看到一些记录在案的流程。这一手段与合作伙伴（比如Tradehill）有着鲜明的不同，Tradehill会更多地专注于高净值市场。它拒绝在没有拿到所有美国国家许可的情况下做生意，并且在解决这一问题的同时已经退出了市场。

由此可见，Coinbase的举动相当大胆。先拿下市场有利于抢占先机；早期参与者可以在监管者入场前，拿下一大块市场份额并建立一个

健康的现金流。以Square为例，他们被佛罗里达州和伊利诺伊州的监管者罚款50.7万美元，因为其没有拿到许可证就开始营业了。但是，到了那个时候，公司已经聚集了3.31亿美元的资金，并且佛罗里达州的罚款（这使得它随后拿到了在佛州的许可证）在那个时候只是被当作做生意的成本了。

Coinbase还有很长的路要走。它在2013年5月成功地拿下了Union Square Ventures主导的A轮价值500万美元的投资。在当时，那是与比特币相关的公司拿到的最大一笔投资，并且这为将来拿到更多的投资做了良好的铺垫。同时，尽管比特币在2014年走势不佳，但Coinbase在2014年中却表现不俗，不仅获得了由DFJ领投、纽交所和美国汽车协会联合服务银行（USAA）和其他投资机构高达7500万美元的投资，还说服了一些著名零售商第一次成为比特币交易的合作伙伴，包括戴尔、Overstock、Mozilla和Wikipedia等。投资者、商户和用户的支持，表明了各方对比特币的信心。该公司此前已经融资3000万美元，其中包括由著名风投机构Andreessen Horowitz领投的2500万美元B轮融资。风险投资公司Union Square Ventures、Ribbit Capital和SV Angel也都对Coinbase进行了投资。它持续地成长着，并和Cashier Commerce签署了一份协议，使后者可以在BitDazzle（这是一个线上的针对对比特币友好的商户的Esty风格的市场）上使用它的商户API。如果监管者真的来找麻烦了，公司希望它已经筹集到足够的资金来应付它们。与此同时，Coinbase将关注交易量的增长层面，通过在仍然是新兴的市场那里获得广泛的关注。这是公司免除了商户的前100万美元的销售处理费用的原因之一。它还将力求关注用户想要什么，这可能会让核心开发团队在开发商户和钱包特性的时候先人一步。

2015年11月20日，Coinbase再次努力推动比特币走向主流，该公司推出美国首张比特币借记卡，也就是Shift Card。它可以让你在任何商户使用比特币——在线或者离线——就像使用任何普通Visa卡一样。想象一下，可以通过它使用比特币来购买墨西哥卷饼，也可以在亚马逊网站

购买电视机。Coinbase表示，该公司用户通过其提供的服务已经创建了200万个比特币钱包。Coinbase还称，Expedia、戴尔、Overstock.com和Stripe都是它的企业客户和消费者。Coinbase的收入来自其平台上对买卖比特币收取一定比例提成。此外，商人首次支付100万美元比特币要向Coinbase提供1%的服务费。Coinbase的业务发展和战略副总裁亚当·怀特（Adam White）表示，他们所做的一切，就是努力让比特币变得更加容易使用，也希望能够非常容易地购买和出售比特币，而主流的比特币借记卡也许是一个关键因素。

根据Coinbase的说法，该卡已经被批准居住在美国25个州的任何人使用，其中包括得克萨斯州、华盛顿州以及新泽西州。尽管也可以在加州使用，但是只能作为“测试版”使用，最高不能超过1000名用户。任何拥有Coinbase账户的人都可以申请新的借记卡。在注册时，必须先验证身份，并且支付10美元的保险手续费。在此之后，只要是从美国的商户手中购买，就可以使用比特币直接进行支付，而没有任何其他的费用（就类似于其他的借记卡和信用卡，手续费是由商户支付的）。如果是用这些卡在海外消费，就必须支付一定的跨国结算费用。当然，你也可以使用这张卡直接从ATM机取出你的钱，资金是来自你在Coinbase比特币账户内的余额，而不是一个银行账户——这也会需要一定的手续费。

对于Coinbase而言，希望让现有的客户开始更多地使用比特币来进行消费，而不仅仅是用于投机。而且新的客户将会被吸引到数字货币领域，因为这些数字货币能够很容易地花掉。而其他一些企业，包括初创企业Xapo，虽然也一直在探索比特币借记卡，但它们只能在海外使用。

有些人担心，比特币让资金流动变得太容易了——尤其是因为人们能够匿名地使用数字货币。有消息称，欧盟正准备打击使用比特币匿名资助恐怖活动。比特币和其他一些数字货币的确可以这样使用，但是这些特性并不能刻画出数字货币的全部。Coinbase新的借记卡将会缓解人

们对于匿名性的关注。因为就像其他的借记卡和信用卡，每个人必须验证自己的身份才可以使用它。就像许多人一样，Coinbase希望将比特币带入到一个全新的领域——主流社会。

四、去中心化交易所

（一）Linq

在2015年下半年，纳斯达克交易所推出了新的针对一级市场的交易平台Linq，该交易平台是基于比特币交易技术，用于一级市场公司的交易。纳斯达克交易所还宣布了对SecondMarket的收购，后者是服务于非上市公司的股份交易平台，曾服务客户包括上市前的Facebook、Twitter（推特）和还未上市的Dropbox（一个提供同步本地文件的网络存储在线应用）等。

纳斯达克首席执行官鲍勃·格雷菲尔德（Bob Greifeld）表示，非上市公司的数量不断增加，为满足他们的需求，纳斯达克将向这些非上市公司提供交易服务，未来这些公司上市时，将为纳斯达克交易所赢得更多的上市业务，同时他认为未来纳斯达克交易所来自非上市公司交易业务的收入将达到甚至超过来自传统二级市场的业务。

纳斯达克交易所称，第三季度来自一级市场的客户增加了20个，使得总数量达到120个，一级市场的业务将成为纳斯达克交易所业务未来增长的驱动力。

纳斯达克区块链战略负责人弗雷德里克·沃斯（Fredrik Voss）确信基于区块链技术所提供的高效率，将能够大幅度提升Linq作为私人股权交易平台的优势。沃斯和全球软件开发总监亚历克斯·津德尔（Alex Zinder）认为区块链具有卓越能力，对于私人股权交易市场而言，最大的好处就是不再需要笔和纸，或者是基于电子表格来记录。

津德尔表示，到目前为止还没有任何技术能够真正让人们远离纸张

作业，而区块链技术将会帮助我们往这个方向前进一大步。现在，传统的手工处理方式往往会留下很大的人工失误空间。

纳斯达克通信专家威廉·布里甘汀（Willian Brigantin）称区块链技术有潜力能够消除这个痛点，因为其最大的“核心优势”就是能够提供一种不可篡改的记录，以及为用户提供一个永久保存的数据链。他们在许多初创公司管理者之间进行调查，绝大部分公司都在融资时使用电子表格来记录股权。为了达到更好的透明性和可审计性，希望今后能够推广使用他们的标准。

纳斯达克私人股权市场是在2014年推出的，这是交易所进入Pre-IPO（上市前）阶段让二级市场进行股权交易最新的一次尝试，这种方式可以一直追溯到1990年。但是今天，有越来越多的初创公司选择保留更长时间处于私人公司阶段（暂时不进入公开发行阶段），这意味着IPO（首次公开募股）之前的交易变得再次令人关注，因为投资者希望能够获得一些流动性，也可以减少早期阶段管理层的压力。

如果仔细研究一下Linq会发现，这是一款较为时尚的产品，它为投资者和企业家提供了一个直观的用户体验。在Linq上，股份发行人在登录后可以看到一个管理控制台来显示估值，包括每一轮投资之后已发行股份的价格，以及股票期权的比例。

所有这些股份数字，包括尚未分配的股份，都通过可视化的颜色块来代表，纳斯达克将该数据称为“股权时间轴视图”。那些已经发生的交易将会在时间轴上显示为“空”，并且变成灰色。用户还可以看到箭头，说明该股份是如何被转移和划分的。

津德尔和沃斯解释道，Linq所做的是，显示在不同时间跨度中企业的活动。每一个单独标志代表一个在线证书。颜色代表某一种特定资产列表，资产类别可以由发行人自行定义，包括股权类型和融资次数。颜色编码的方式，能够非常直观地通过开放资产协议（Open Assets

Protocol），来显示区块链技术是如何通过相应条款和条件来创建独一无二的资产。这些可视化的表现都是完全真实的，只要这些是记录在区块链之上的。股权时间轴上显示的是最有价值的东西，它能够将显示信息可视化，并且表明交易和来源。



图4.2 Linq产品界面（Linq上的管理控制台上的“股权时间轴视图”）

Linq力求企业家能够更简单地通过对资产表格进行数据分析，来提供更直观的可视效果，否则很容易会被电子表格所湮没。例如，创业者可以在交互式股权时间轴上，显示个人股份证书是如何发给投资者的。有效的证书和取消的证书都有不同的显示效果，前者还会显示诸如资产ID，每股价格等信息。

初创公司使用平台还可以通过时间发行日期来查阅证书，包括查看最多或者最近的证书，并且只要点击一下，就可以查看哪些投资者在企业内持有最多的股份。

在其他地方，创业企业可以评估某单一投资者在企业中所持有的股份。投资者可以面对类似于事务ID，为那些正在追踪初创公司进展的投资者提供足够的透明性，还强调他们使用了新技术来创建证书。

津德尔和沃斯进一步暗示了某些非技术性的工作还在进一步展开，

来帮助Linq的创建，并且表明最终产品将会比设计的更加优秀。因为他们需要一件可以使用的漂亮产品，需要能够为他们所有的客户提供，用于解释该产品的深层次功能。

Linq正在被6个创业公司和他们的投资者试用。这几个有限的参与公司，需要能够通过合法的电子凭证来代表他们股份的所有权，纳斯达克称如果一些初创公司有着复杂的股权结构，便会让迁移过程变得更长。并且，法律程序会需要在某些州的公司与其股东进行沟通，他们将会发行“非凭证股份”，意味着不再有代表股份的物理证书。在把Linq推向现在所有客户，来进行更大范围内的测试之前，这些股份流动将仅仅局限在初创公司之内，他们会有权但不是有义务对投资者开启流动性（交易股份），现在就可以通过Linq来完成。

根据纳斯达克的阐述，他们的目标是让整个流程变得更加简单，以及区块链技术能够让它变得更加灵活和方便，并且获得更广泛的应用。他们现在做的事情，就是创造结构化流动性，在整个过程中减少摩擦，客户就会获得更多的流动性。纳斯达克还暗示Nasdaq Linq也许有一天会演化成一个独立的产品，也许甚至会投入到公开股票交易所中。

（二）TØ

1.Overstock

Overstock.com, Inc.（纳斯达克代号：OSTK）是一家位于美国犹他州盐湖城的在线购物零售商，以折扣价格销售家具、地毯、床上用品、电子产品、服装及珠宝等各类产品。《福布斯》杂志将Overstock评选为2014年最值得信赖的100家公司之一。

Overstock于1999年上线，目前共有1300多名员工，是2002年上市时

的6倍多。截至2016年1月3日，公司的总市值为3.1亿美元。最近一个财年营业收入为15亿美元，与索尼、惠普等供应商建立了良好的关系。此外，Overstock还有汽车、旅游、保险、B2B（Business-to-Business）等业务。目前，Overstock产品已销往全球180个国家和地区。

从2014年1月9日开始，Overstock正式接受比特币支付，成为比特币历史上的关键一刻。这是公司首席执行官帕特里克·拜恩（Patrick Byrne）推动的结果，在帕特里克·拜恩看来，只有比特币才能改造华尔街，推动金融改革，从而避免下一场经济大衰退。

Overstock与Coinbase协作，通过后者的交易平台接受比特币支付结算。在不足两个月的时间里，Overstock共获得超过100万美元的比特币交易订单，其中，平均每比特币用户的消费水平为226美元，高于普通用户168美元的平均消费水平。在所有使用比特币支付的用户中，有超过一半（约58%）的用户为新注册用户，这些新用户此前从未在Overstock上进行过任何消费。

在Overstock接受比特币付款后，又有多家美国大公司相继跟进，包括戴尔、Dish Network和新蛋。另据比特币数据提供商CoinDesk统计，目前全球有6万多商家接受比特币付款。

据帕特里克·拜恩透露，比特币等数字货币的支付成本远低于传统渠道。例如，比特币支付服务提供商Coinbase仅向Overstock收取不足1%的手续费，有时甚至接近于零。而信用卡公司的交易费比率通常为3%。Overstock还于2014年9月中旬接受国际客户的比特币付款。另外，该公司还将从比特币销售额中拿出4%，用于推广这种货币。

2.裸卖空

帕特里克·拜恩自称是巴菲特的门徒，拿到了哲学系博士学位，专注于经济学和法学的他还倾向于自由主义，多年来他一直想要改革华尔

街，在他看来，区块链也许是可以实现他愿望的一种东西。作为一位奉行自由主义的哲学家，他经常在自己的项目理念中传达他的自由主义思想和奥地利经济学派思维。

拜恩提出，区块链技术之于资本市场，即互联网之于消费者，它的设计提供了一种安全、透明并且可靠的方式，能够记录谁在任何时间段拥有了特定的证券。在拜恩看来，它可以取代传统证券交易所运行的旧系统。长期以来他一直认为，华尔街金融系统的不透明导致出现诸多漏洞，这些漏洞常常被金融机构利用来牟取暴利。其中一个漏洞就是“卖空”投机行为。

卖空是指股票投资者在某种股票价格看跌时，便从经纪人手中借入该股票抛出，日后该股票价格果然下落时，再以更低的价格买进股票归还经纪人，从中赚取差价。而在“裸”卖空（无担保卖空）交易中，卖家不能及时借到证券并在标准的三个交易日结算期间向买家交货的话，将导致该证券“未交付”。

“裸”卖空并不一定违反联邦证券法或证券交易委员会的规定。证交会指出，“在某些情况下，‘裸’卖空有利于市场流动性”。2008年，美国证券交易委员（SEC）会出台规定禁止美国国内“滥用‘裸’卖空”的行为，因为这种行为经常被认为与价格操纵、拉低股价有关。

拜恩指责数家银行和对冲基金在过去串通压低Overstock的股价，最近Overstock与美林证券在一起纠纷上达成了和解。拜恩声称，尽管法院在其裁决中已经发现大量证据表明，Goldman Brokerage（高盛经纪）本身就从事欺诈，但高盛却已经在调查期间掩护自身安全撤退了。但这件事并没有让他太担心，因为公司在加密事业上做出了自己的努力。

3.10系统

拜恩所提到的他们在加密事业上的努力之一，便是在过去的一年

中，Overstock开发的基于区块链的“TØ”（念T fita）证券交易平台。区块链基本上是一个横跨全球的庞大分布式数据库，它是由独立的计算机负责运行维护的。有了比特币这种代币，这个账本可以跟踪比特币网络上的交易，此外，它也可以用于跟踪任何其他有价值的交易，包括股票、债券和其他金融证券。TØ是比特币区块链在金融领域中的应用。Overstock表示：“TØ使证券交易变得更加公平、透明和方便所有市场参与者的参与。”

对于Overstock而言，尽管在其平台上发行股票还是一个有待求证的想法，但是从根本上来说，TØ主要工作的内容是进行“交易结算”。特别是面对传统股票交易市场的现状，实行的是交易日加三个工作日（T+3）的结算机制，其中的三个交易日，是交易需要三天时间来完成证券的结算工作。而如果使用区块链技术将能够实时结算，几乎可以在交易完成的瞬间就完成结算工作。

TØ的平台使用了彩色币技术，它允许使用很小一笔比特币来追踪资产所有权的机制。例如，一个彩色币可以用来作为一个标记，证明某个人持有Overstock的股权。这个技术将会在比特币区块链上进行，并且由分布式总账的区块链技术来确保安全。

拜恩指出，TØ的一切技术都是建立在分布式、加密保护的账本上，任何人都可以访问和审查这个账本，确保整个市场的公平性。打破华尔街和其他行业的关键不在比特币，而在区块链技术。有了一个自动共享、防篡改的数据库，存储数据将不再需要烦琐的手续和清算机构。为向人们展示TØ系统，拜恩在2015年6月购买了50万美元Overstock发行的债券。在随后的一个月，Overstock宣布向FNY资本的子公司（纽约贸易公司FNY账户管理公司）出售了500万美元的“加密债券”。

总部设在纽约的Clique对冲基金，利用这个系统借来30只组成道琼斯工业平均指数的股票。该交易价值1000万美元，都被记录在区块链

上。与拜恩一起创立TØ的约翰·塔巴科（John Tabacco）表示：“这是一笔真正的交易。”他同时还透露，TØ在过去的两周内一直促进股票的借出，已有5个客户借出了股票，包括Clique基金。

区块链的优势在于它可以简化交易流程，提供更加可靠的交易记录，它也是拜恩与“裸”卖空及与美林证券“战斗”的一个关键“武器”。2015年10月15日，TØ宣布Clique基金交易已经在其平台上测试了一种新的加密资产，即预借保证代币（PAT）。该团队已经成功在一个交易商进行卖空之前，利用比特币区块链记录下了符合美国证券交易委员会规则的商号证据。

拜恩指出，他们推出的预借保证代币是为了解决权益所有者的问题，通过将权益所有者手中的资产放到透明的市场中来保障其收益；这也将能解决卖空者的问题，只要他是在透明的市场中借贷；还能够解决监管机构所面临的问题。他同时也承认，相比10年前，监管者现在对这种投机行为的打击力度更大。不幸的是，这当中还是存在“害群之马”，必须要把这些“害群之马”消灭掉，这正是要推出预借保证代币的目的。

SEC规则SHO（证券卖空规则）鉴于1938年首次通过卖空规定以来的众多市场发展情况而更新规定，解决持续未交付和潜在的滥用“裸”卖空的问题。拜恩明确表示在原则上同意SEC，在卖空原则上并不反对走法律程序。

利用区块链实施的第一个卖空测试是十足的壮举。当全面投入运营后，该团队称，该服务将在一个“不透明的股票借贷世界”中提供前所未有的透明度。在奉行自由主义理念的拜恩看来，TØ平台是第一个“华尔街式”概念的范式。随着完成卖空测试，表明该系统确实可以运作，不过这一平台能打破多少传统金融服务，只有时间才能证明。区块链是人們所遇见的最重要的金融发展成果，当其他人还在观望这一新技术能否引进的时候，TØ已经开始行动起来，决心用它来对抗证券借贷中的“暗

箱操作”行为。

根据Overstock2015年的第四季度季报，2015年前面三个月时间里，这家在线零售公司在区块链证券项目上已经投了320万美元。该季报说明它可能将会投资800多万美元用于发展Mdici，这是它旗下使用区块链技术进行探索的子公司，而区块链交易平台TØ就是它的核心项目之一。为此，首席执行官拜恩在给他股东的信中这样解释说，Medici在2015年的成本接近800万美元，当你增加许多要执行多项任务的员工所提供的开销和服务，以及其他负荷因素时，2015年的真实成本将会显著增加。拜恩建议说，该公司正在寻求将其区块链交易平台从Overstock自己的电子商务设施中拆分出来以获得更广泛的应用，使股东的利益最大化。

为了努力进军金融行业，TØ平台在2015年10月以3030万美元的价格收购了华尔街经纪公司SpeedRoute来协助推进其区块链交易平台。拜恩表示，这是一个能够连接美国11个交易所和25个非公开资金池的路由服务，它已经是美国市场中一个重要的节点。如果需要把区块链引入到华尔街，不是为了建立一个信息孤岛，而是为了让大家能够接受它，所以需要购买美国市场体系中的一个节点，然后在上面建立加密技术，这样就可以符合所有的监管规定，并将其视为互联网金融技术。他们并不希望成为类似于Mt.Gox这样的公司，想尽一切办法来规避监管，而是能够在和Medici相关业务上展开进一步的投资和收购。

4.SEC批准

在2015年12月中旬，SEC已批准在线零售商Overstock.com通过比特币区块链来发行该公司的股票。据Overstock提交给证券交易委员会的S-3申请，该公司希望通过区块链来发行最高5亿美元的新证券，包括普通股、优先股、存托凭证、权证、债券等。

S-3申请是一个证券登记表格，允许企业以简化流程来发布可公开可交易股票。不同于S-1申请，这需要对公司计划将持有的股票进行IPO

而进行全面备案，而S-3是根据1934年证券交易法案（Securities Exchange Act）提出的，对已经符合一定资格的企业而言特别要求的是，一个公司需要至少有12个月对SEC进行档案报告，才有资格提交S-3申请。

此前，Overstock已经使用区块链来发行私募债券，这不需要监管机构的批准。而现在，SEC已告知Overstock这家公司，它可以以同样的方式来发行公开交易证券。根据Overstock提交的公开文件，SEC已经批准了修订后的S-3申请，允许该公司通过区块链来发行公开交易证券。拜恩从未确认发行公开证券的具体时间，但他表示这将会是他们在2016年最为首要的事情。

Overstock将通过旗下的TØ区块链平台来发行这些公开交易证券，它也计划为其他公司提供这种“加密证券”服务。需要注意的是，选择通过TØ平台来发行公司股票的企业，都需要得到SEC的单独审批。

对Overstock的批准毫无疑问会成为某种催化剂，因为它计划向其他企业提供该技术，帮助他们发行自己的加密证券。如果该技术在公众领域能够惊艳亮相，也许能够迫使其他公司也采用区块链技术来发行证券。但是，不能确认的是SEC是否还会继续批准这样的情况。

区块链技术有利于大幅度削减发行、追踪和交易加密证券的成本。它在金融市场中提供了一个完全透明、安全、可靠和快速的基础设置。这项比特币的底层技术也许还能够防止市场操纵行为，并且成为一种自动运行的系统，从而完全取代传统交易所。

目前，TØ计划通过区块链来帮助其他公司管理金融证券，并且已经在进行中，除了发行私募债券，TØ还提供了一种工具可以让公司通过区块链来进行股票的借贷。这一设计瞄准了美国股票借贷9540亿美元的市场，消除传统的中间商，并填补股票结算的漏洞，允许交易者进行股份的“裸”卖空交易。根据Overstock和TØ的说法，一些对冲基金和其他组织

已经测试了这种系统。

（三）BitShares

1.简介

BitShares是一个工业级的开源去中心化金融智能合约平台，该平台基于Cryptonomex公司研发的Graphene（石墨烯）技术开发。Graphene是一个开源开发工具包，同时也是实时区块链的技术实现，旨在实现一种区块链技术或协议。然而与具体的区块链整合后，比如BitShares，它逐渐进化为一种生态系统。

BitShares内置了一个类似于上证所或者纳斯达克这样的去中心化交易所系统，和这些传统交易所相比最大的不同是，由于BitShares是完全不依靠任何人而在自动运行，因此在里面所有交易的资产、产品可以由任何人创建并交易。

传统证券交易所的流程是，任何公司如果要将自己的公司股权在公开市场上发售，也被称为IPO过程，首先需要把自己公司的所有资料交给交易所或者相关审核机关进行审查，通过以后寻找券商进入一级市场进行销售，完成之后就可以在相关证券交易所中开始交易股份。这其中的手续之烦琐，成本之高昂，相信即使不是在这个行业内的人都是很清楚的。但是去中心化交易所则完全颠覆了整个过程。

任何人只要缴纳一定的手续费都可以在上面发布要交易的资产，不需要任何其他成本，既不需要去购买服务器，也不用学习什么代码，只要设定自己需要发布资产的名称、描述、代码、数量、交易手续费等就可以。完全由创建者自定义交易手续费，只要在系统中进行交易，系统会按照创建者的设定把每笔交易手续费打入创建者的账户中。

BitShares为商业而生，如同Bitcoin为货币而生。两者皆采用分布式共识机制来创建具有全球性、透明性、可信赖的、更高效的系统，更重要的是能为企业带来更多利润。

2.系统优势

首先就是规避了大多数法律问题，几乎在全球各国建立集中竞价的交易所都是有牌照的，必须受到该国法律法规的监管。但是司法监管的前提是有监管对象，而对象不外乎是人或者是机构这样的法律实体，而BitShares仅仅是一段程序，并且它是存在于互联网上的一段程序，并没有特定的国界，所以如果所有人都在BitShares上进行交易的话，这个行为能够规避大多数国家的法律。而且和比特币一样，基于区块链技术的程序一旦部署在互联网上，即使是创始人也无法改变。就像即使我们找到了创立比特币的中本聪，即便是肉体上消灭中本聪也不会影响到比特币的运行。

其次是解决了充值上的问题。交易所如何进行充值对于数字货币行业内的人而言一直是充满困扰的问题，并且随着第三方支付牌照被控制在一定数量之内，它们的地位变得越来越重要，它们对商家的审核门槛也变得越来越高的。而BitShares让充值不再依赖于一个单个中心化的机构来处理，几乎人人都可以成为承兑商，人人都可以来交换人民币/BitCNY。考虑到目前几乎所有的国家都将BitCNY这些数字货币定义为商品（BitCNY作为一种数字货币，中国五部委有明确解释，个人有买卖数字货币的自由），无论是成为承兑商还是与承兑商进行交易都没有任何的法律问题。

技术门槛也是困扰许多非技术人员的因素。当许多人还在考虑建立一个交易所应该组建一支如何强悍的技术团队时，BitShares几乎已经将所有的事情帮你搞定了。你不仅不需要考虑技术团队、代码，或者连服务器都不需要。只要下载BitShares的客户端，或者是打开BitShares的网

页就可以在上面完全根据你的需要来创建资产凭证，这个资产可以是论坛的积分/代币，也可以是公司的优惠券/奖券，甚至还可以是某个公司的股票/债券。

由于身份安全往往是和资金监管相关联的，而传统的交易所会要求用户提供各种身份证明，在这种情况下，交易所对每个用户的资金情况了如指掌，甚至有些交易所会因为其他原因私自冻结扣押用户资金。在这种情况下，大多数用户都处于一个相对弱势的地位，而这一切在BitShares系统是绝对不会发生的。BitShares把资金进出的功能交给了承兑商，而承兑商和交易是完全没有关联的，在这种情况下你不用担心自己的资金和交易记录会被追踪，所有的资金和交易完全由你操控，更不可能出现冻结之类的情况。

最后，由于BitShares本身就是在互联网上运行，因此其本身是没有国界的。除了有中国的人民币承兑商之外，还有国外的美元承兑商。每个人都可以随时随地下载客户端进行交易，使用者可能来自全球互联网每一个角落。

3.应用场景

论坛或网站的管理者往往会需要发行自己的代币，这时就可以巧妙地利用BitShares来完成。一些论坛管理者如果不愿意直接用自己的私人账号收费，那么他完全可以先在BitShares系统上创建自己的代币凭证（进入“比特资产”后，点击创建“创建新的比特资产”），然后直接在论坛上收取BitCNY，并且收取后根据自己的规则将创建的代币凭证发给用户们，或者也可以直接在BitShares上销售这些代币凭证，需要的论坛用户都可以随时购买。

更进一步来看的话，如果该论坛愿意和用户们共享发展的收益，他也可以在BitShares上发行自己的论坛股票（凭证），每个购买股票的用户可以获得论坛每月收入的若干百分比，论坛会每月将这些收入按股票

比例通过系统发送给股票凭证持有者。这样的话，愿意购买论坛股票的用户则变成了股东，他们不仅可以在BitShares买卖股票并且获得收益，还能够自愿成为论坛的推广者，因为论坛的收入越多他的收益也就越高。而在没有BitShares系统的情况下，这些都是很难实现的。论坛不仅可能需要投入力量来建设这么一个交易所，而且也不能做到像BitShares这么客观的第三方（无法作弊），每个用户可以公开监督社区的收入，并且能知道论坛会不会私下增发股票之类的欺诈行为。

我们可以再扩展一下我们的想象力，如果某个YY（同音歪歪，一款免费的团队传音软件）主播（或者是网络红人Papi酱）愿意通过出让自己未来10年收入的一部分，来公开募资让自己现在获得启动资金投入学习到学习和装备购买上，那么她也可以在BitShares发行自己的个人股票（理论上只有公司才能发行股票，这里是一个比喻），如果大家愿意看好她的话，都可以购买她所发行的股票，而她可以让YY每月出一张收入证明，并且将收入的一部分按股票比例发送给持股者。这就等于把这位也许很有“星途”的YY主播证券化了，她通过预先售出自己未来收入的一部分获得了现在的启动资金，而投资者能够进行可量化回报的投资。当然，对于这位主播而言，更有价值的是获得了大量的股东，这些股东会自愿成为推广她的粉丝，而粉丝可以在推广明星的同时获得收入回报，形成一个良性的循环。

从上面的例子来看，其实已经把“人”当作了一个公司来IPO，那么真正的公司也可以通过这种方式来筹资。当一些初创公司需要资金的时候往往会求助于VC或者天使投资人，他们之所以不向普通人求助是因为即使普通投资者愿意投资，如果金额太少的话，就意味着他们需要花大量的时间向普通投资者募资。当然现在我们有了一种全新的方式，那就是众筹平台，但是现在的众筹平台仅仅是解决了融资者能够快速面对大量普通投资者的问题，而没有解决投资者容易退出的问题。对于投资者而言，没有什么比让自己的投资能随时退出更重要的事情了，不管你的投资标的在账面上能够涨成什么样子，关键是要能够随时买入和卖

出，而现实是只有证券市场能提供这样的流动性，我们不能私自搞交易所，但是大家需要明白，持有股份是合法的，交易股份也是合法的，而需要牌照的只是集中竞价场所，那么对于一个去中心化交易的市场而言，这一切都迎刃而解了。公司完全可以在BitShares发行自己股份的权益凭证给那些投资者，这样投资者就能够在BitShares平台上进行自由的交易而不触犯任何法律问题。

BitShares取代传统交易所仅仅也是开始，如果你是一个商家，你可能经常需要发放优惠券或者奖券，如果通过BitShares系统（API）来发放，不仅能确保整个环节公正透明，并且这些优惠券能够很容易地购买和兑现，特别有趣的是那些不需要优惠券的客户可以把拿到的优惠券在BitShares上卖掉，对于商家来说更希望客户如果不需要可以赠予或出售给需要的人，而不是直接扔掉。在过去要实现交易功能对于商家来说不值得投入巨大的技术开发力量，而对于想出手优惠券的用户来说，如果优惠券面额不大的话在淘宝上销售既费时又费力，况且买方也不知道到底购买的优惠券是否真实。这一切通过BitShares系统都可以迎刃而解，因为在BitShares上的凭证是完全无法伪造的。

如果你是一个艺术品收藏家，你手里有些价格昂贵的名画，平时这些名画肯定是放在保险箱里，而现在我们也可以把这些艺术品直接份额化，然后每个人持有一部分进行交易。是的，我想你肯定想到了著名的天津文交所，同样也是有政府监管等问题，各地的文交所被陆续关停。就像前面所说的，任何集中竞价的交易所都需要符合政府监管。需要再重申一下，其实持有一部分艺术品是合法的，交换这些份额也是合法的，只有集中竞价是需要牌照的，而BitShares又一次能够完美地解决这个问题。

如果你有一个P2P借贷交易所，在BitShares的平台上能够让P2P借贷资产变得更加具有流动性，不仅在交易中所有的数据无法篡改和透明，更能吸引来自全球的投资者。由于BitShares平台是完全没有国界的，因

此在BitShares这个平台上可以非常容易地进行货币交换。目前国内的年化收益率最低也有3%~5%，而在P2P借贷的网站上一一般年化收益率都在10%以上。但是全球其他国家的平均利率非常低，不少国家的利率近乎于零，甚至有些国家的利率为负数。因此，从全球来看这存在一个非常大的套利空间。而在BitShares上就可以很简单实现这样的套利模式。

在BitShares系统中，预测市场也很容易实现。一个二元预测市场有一个介于0~1的“价格”，代表一个未来时间的两种可能的结果。需要做的只是创建一个预测市场资产，并填写准确合适的描述，任何人都可以通过锁定抵押物来发行该资产。

所以，预测市场资产是一种特殊的市场锚定资产，不需要强制平仓和强制清算，因为无论处于什么价格，所有的仓位总是满额抵押的。当预测事件尚未发生时，该资产的价格反映了市场认为该事件结果发生的概率。当事件发生结果公布后，发行人可锁定交易，并根据事件结果“价格”发起全局清算。预测正确的参与者因此将获得利润。预测市场可以是非常安全的，比如发行人账户可以是一个多重签名的账户，持有人包括许多独立并值得信赖的个人或企业，由他们共同参与管理流程的各个环节。

此外，BitShares提供稳定的市场资产，例如BitCNY，它的价值源于通过复杂的市场引擎去跟踪真实的人民币法币，因此它拥有价值相对稳定的特性，例如1000BitCNY即使存储三个月或者半年，它的价格也不会像比特币那样大幅波动。这样的特性解决了比特币长期存储时可能出现的价值损失问题。而BitCNY更大的作用是帮助人民币国际化。人民币国际化是指人民币能够跨越国界在境外流通，成为国际上普遍认可的计价、结算及储备货币的过程。人民币境外流通的扩大最终必然促使人民币国际化，使其成为世界货币。

五、去中心化电子商务

OpenBazaar（公开市场）是为网上P2P交易创建的去中心化网络的开源项目。在OpenBazaar平台上买卖双方使用比特币进行交易，没有费用，而且不会受到政府监管机构的审查。简单地说，它就是eBay（易贝）和BitTorrent结合的产物。

大多数人已对标准电子商务模式非常熟悉了。一家公司——如eBay，亚马逊或者淘宝，它们都会有一个流行的网站，人们会通过这些网站购买或者出售东西。这些公司都是直接控制着网站上的交易的，你不会在这些网站上看到非法或者非道德的商品，因为这些公司不允许这样做，他们会删除那些非法的清单。这种模型是一种中心控制的模型，因为有一个中央权力机构可以去决策和控制发生的事情。

现有的电子商务模式即意味着使用中心化的服务。eBay、亚马逊和其他大公司对卖家实施严格监管，而且收取不菲的费用。这些公司只接受类似于信用卡和PayPal这样对卖家和买家都收取手续费的支付方式。他们需要用户的个人信息，这些信息可能被盗取或者卖给其他人，用于精准投放广告或者危害更大的滥用。因为电子商务公司和政府会审查所有的交易商品和服务，所以买家和卖家不能总是自由地进行交易。

OpenBazaar为电子商务提供了另一途径，它把权力归还到用户手中。OpenBazaar将卖家和买家直接联系在一起，不再需要中心化的第三方来连接买卖双方。因为在交易中不存在第三方，所以不存在交易费用，没有人能够审查交易，而且公开个人信息的决定权在用户手中。

独立公司OB1成立于弗吉尼亚州，目前是OpenBazaar平台上完成度最高的第三方提供商。作为建立在OpenBazaar框架上的增值服务业务，OB1最初专注在以下三个核心方面。

其一，主机解决方案：OB1为提供一个易于使用的第三方解决方案，正在与云服务器提供商Digital Ocean进行合作。

其二，仲裁服务：OB1希望提供标准合同服务，即在法院具有法律效力，尤其是对高端行业，包括房地产。他们的目标是为不同的需求、商品和服务，提供一个合法的框架以及不同的合同类型。

其三，买家保护：OB1的目标是提供第三方保存服务，以及为买家和卖家提供保险。

当前，OpenBazaar项目所面临的最主要问题是用户的非法交易，由于用户使用强加密软件Bitmessage、PGP，以及数字货币，OpenBazaar将无法探听用户的交易。OpenBazaar也无法收集发生在平台上的活动数据。布莱恩·霍夫曼（Brian Hoffman）曾表示，他的团队不认可也不支持将OpenBazaar用于非法目的，如果平台的大趋势是成为非法用途的“温床”，那他将远离这个项目。

OB1不会将OpenBazaar协议给任何机构或个人，用于非法用途的用户提供增值服务。棘手的问题是，OB1是如何支持一个开放的协议的，因为他们不受控制，也不鼓励和赞同，甚至是促进该协议的滥用。

OpenBazaar一再重申并不想创造“3.0版本的丝绸之路”，开发负责人布莱恩·霍夫曼表示，公司绝不会姑息任何对平台的“不当使用”，然而由于其系统架构分散，又明确表态不干预用户，如何防范违法交易这一问题尚无结论。OpenBazaar将对在线商务产生革命性的影响可能没错，但该公司的商业模式也可能成为美国技术产业的潜在威胁。OpenBazaar的技术本质上是野蛮生长且不可控的，一旦最后为恐怖主义所用，当局可能将启动更为广泛的打压行动，将执法者认为妨碍其职责的其他技术也列入打击范围。

六、公证和鉴证服务

（一）Factom

Factom是一个P2P网络系统。网络系统中的高端服务器先创建数据链，然后对这些数据进行加密处理，再利用Merkle root将其加入比特币的Blockchain里。第二代数字货币中一个里程碑式的成果就是提出了利用Blockchain，以加密的形式来确保信息准确性这一概念，并且在过去的几年里这个概念得到不断完善。然而，Factom公司另辟蹊径提出一种比特币网络之外的新系统。但是这个新系统仍然需要依托比特币散布全球的电脑运算能力，使得这些加密认证的消息是对外透明、对外开放的。如同Factom团队所说，近期新的比特币应用都在现有的机制基础上加入了新的机制，以提高交易透明性。公司总裁彼德·卡比（Peter Kirby）在Reddit一个有问必答环节中强调说他们团队已经在和一些有意向的第三方接洽，这些第三方机构认为该公司的设备可以解决他们的问题。彼德·卡比认为，Factom公司的首要任务是使得比特币交易更真实透明。这些真实性经得起任何检验——你可以对任一时刻进行的任一交易进行细致入微的检查。

保罗·斯诺（Paul Snow）、布莱恩·比尔瑞（Brian Beery）、杰克·卢（Jack Lu）、戴维·约翰逊（David Johnston）及彼德·卡比联合发布了Factom公司的白皮书，这份白皮书引用了许多著名评论家的看法，包括以太坊的创始人维塔利克·比特林以及比特币开发专家卢克·达什尔（Luke Dashjr）。他们在书中探究了一种新系统，使得与比特币相关的尤其是与所有权相关的记录过程，由分散到数字化，由手动到自动化；也构思了一种概念型网络框架，这个新系统可以确保并提高留存在比特币Blockchain里的交易记录、文件及其他一些重要数据的准确性。白皮

书作者们说，这种做法的优点就是可以利用比特币的叠加处理能力，同时可以避免对数据的超量运算处理——所谓的区块链膨胀问题。

尽管这份白皮书承认还有许多要点正在开发中，包括这个新系统的协调协议，但不可否认的是，Factom革新了当时整个世界对数据的记录方式，并利用比特币区块链技术来保护数据安全。Factom称他们所采用的方法是可以解决一些危机的，例如美国经济萧条过后连锁产生的抵押贷款债权危机。在经济萧条过后，原先在纸上的所有权记录在电子交易中不幸丢失，从而导致许多地区的房屋所有者被错误地剥夺所有权。直到现在，许多人还因为这个记录丢失而面临法律问题。

Factom利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式。人们能够利用Factom的区块链技术帮助各种各样应用程序的开发，包括审计系统、医疗信息记录、供应链管理、投票系统、财产契据、法律应用、金融系统等。开发者能够创造新的应用程序，并把数据保存在区块链上面，同时不用受到直接把数据写入比特币区块链的各种限制：例如写入的数据速度、成本、大小等。

Factom维护了一个永久不可更改的、基于时间戳记录的区块链数据网络，大大减少了进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。商业社会和政府部门可以利用Factom简化数据记录的管理，记录商业活动，并解决数据记录安全性和符合监管的问题。

（二）Everledger

Everledger是一个永久存在的账本，用于保存钻石证书和相关的交易历史，为保险公司、持有者、索赔者以及执法集团提供检验服务。

Everledger通过区块链来追踪每颗钻石，从矿山开始一直到消费者，甚至更远。使用区块链技术消除钻石诈骗，并希望最终使用该技术

背后的数字货币技术，以解决保险欺诈的行业问题。这将解决长久以来保险行业内长期存在的问题，并且每年将会节省超过3亿英镑的资金，及有效解决钻石检测冲突和保险欺诈。

其官网的数据显示，Everledger在区块链上已记录的钻石达到了575774颗之多，Everledger通过Eris Stack平台，将自己的私有链和比特币的公有链结合起来，完成了一种混合模式，使之既可以享受到公有链带来的安全性，又可以实现私有链的复杂性和智能合约。

如果Everledger有一个5克拉的钻石，就能捕捉到刻在石头上的序列号，大部分钻石都具有4个C（切割、清晰度等）中所描述的序列号。Everledger就不仅是4个C，而是Everledger再取40分的元数据组成的钻石。实验室检查房间里的石头，它们有效地将每个钻石数字化..... Everledger采取所有这一切和序列号及4个C，然后把所有的信息记录在区块链上。

大多数钻石是通过纸或类似物的方法检测，它的认证可以很容易地被篡改。伦敦是一个主要的钻石交易中心，而欺诈问题是导致伦敦钻石市场损失数十亿美元的一个重要原因。如果是一个没有注册的钻石，那么被犯罪分子利用的风险会很高。没有人知道你的石头是从哪里来的，如果你真的把它卖掉了，世界上就没有人能告诉你它其实是被人偷走的。

当然，也可能通过重塑石头来扭曲其“数字指纹”，但钻石很难重塑，因为数据指纹包括了其各部分的总和。钻石重新切割过程会造成大量的浪费，因此，任何企图改变钻石，或将一个钻石拆分成两个的行为，都会大大降低其价值。除了防止欺诈之外，了解一颗钻石的来源、年龄、历史可能也是一件非常有价值的事情。

除了钻石以外，该公司还“积极追求”在奢侈品空间的其他机会。许多贵重物品，从手袋到船，都可以配备RFID（射频识别）标签技术。

奢侈品是一个很大的类别，有很多的物品、资金和跨境交易都可以放在区块链，它是一个全球性的业务。

Everledger总裁琳恩·坎普（Leanne Kemp）表示，保险市场是他们的主要目标之一，他们不会把区块链技术局限在某一个特定类型资产中。

（三）Stampery

区块链初创公司Stampery的目标是为用户提供生成安全、可靠和无可辩驳的存在性证明服务以及保证用户的文件和数字通信的完整性。

Stampery表示已经开发出了基于区块链技术的产品，并已投入运用。并将公司产品整合进广大用户所使用的系统中，已经推出了产品与Dropbox、Box等整合。Stampery的愿景是未来任何需要公证的地方都能使用他们的产品。随着未来越来越多的快速和自动化数据公证方式的出现，传统公证方式将会成为沧海一粟。

作为非金融的区块链应用，Stampery利用区块链无法篡改的属性为所有已经发生的事情生成可靠和永不丢失的存在性证明。Stampery所生成的存在性证明、完整性和所有权在全世界都是有效的、不可改变的，并且可以在几秒内通过任何独立的第三方进行验证。这无疑是革命性的成果，因为今天的数学科学使我们不必依赖任何一个中央机构就可以验证任何发生的事件。

Stampery利用比特币区块链技术解决了数据的认证问题，它允许个人和公司证明任何类型的数据，生成精确、可靠和不可更改的存在性证明、完整性和所有权。任何人都可以免费访问、注册和使用Stampery的服务，使用StamperyPRO计划的用户需要每月支付999欧元，Stampery将为他们提供每月验证1000份文件的服务。

Stampery原创可扩展性解决方案允许Stampery技术与其他拥有大量用户的服务相结合，例如Dropbox，已经有400万用户。Stampery已经开发出了解决可扩展性问题的解决方案，目前正在为该项技术申请国际专利，这项技术可以实现在几秒内验证数百万份文件。

Stampery团队目前正在开发他们的第三个项目，并且该团队从1000多家初创公司中脱颖而出，受邀在旧金山举行的Tech Crunch Disrupt Startup Battlefield大会上做项目路演。

2015年5月，他们推出了该产品的测试版，并多次参加国际密集加速器项目“Menorca Millennials”。

2015年11月，Stampery宣布完成了一轮60万美元的融资，由Draper & Associates领投，区块链资本公司Blockchain Capital和天使投资人迪·安·艾斯诺尔（Di-Ann Eisnor）也参加了该轮投资。同时，Draper & Associates也是特斯拉、百度以及Skype的投资者。

七、开发平台

（一）Blockstream

Blockstream是业内第一家旨在扩大比特币协议层功能的公司，也就是侧链（sidechain）的扩展机制，公司的重点是允许各种创新在一个开放、可互操作的平台上发生。

Blockstream两轮融资共计拿到了7600万美元。迄今为止，该公司的标签技术一直是它的侧链产品，目前正处于测试当中，这种技术可以将资产从一个区块链中转移到其他的区块链中。而鉴于私链和许可链最近引起的关注，Blockstream试图强调，可互操作区块链将为比特币网络添加功能性。公司主要致力于开发开源比特币区块链的技术，因为比特币区块链迄今为止还是“最成熟、最安全”区块链服务的基础设施。

他们的团队中有比特币专家、密码学家、密码学朋克、企业家，还有来自商业、政策和开源社区的领导者。Blockstream的团队中有多位都是比特币协议的资深开发者，因此团队本身具有极强的技术背景。Blockstream是一家以营利为目的的公司。他们相信这一致力于用密码学实现无须信任技术的行业还有巨大的空间（不仅只有比特币，而是通用计算）。创建一个中心化的系统越来越容易，但创建一个无须信任的系统所需的技术却非常匮乏。

他们认为为了激发密码学货币的全部潜能，需要一种建构合理和无须许可的扩展比特币的方式。作为以数字形式存在的、独立于任何政府和机构的新型货币的比特币，在发布以后的五年多时间里，给了人们许多启发和灵感。比特币使金融交易不再需要信任任何第三方。

比特币是第一个建立在加密和匿名的密码学朋克技术上，并取得巨大成功的数字货币。但必须承认的是，比特币本身还有很多的局限性。出于安全原因，比特币开发的速度还非常保守，因此作为一个整体的比特币系统，其创新速度也是非常保守的，目前所有的用户必须分享一个单一系统。

由于保守，许多对比特币必要的修理和被广泛期待的性能提高目前没有得到实施。比特币需要提高的方面包括：协议简化、扩展性、性能和安全性、原生支持多种资产类型、更多的交易类型和加强隐私和可替代性。针对这些问题，侧链可以起到缓解的作用，多个侧链共存是可能的，侧链可以具有更大的区块大小和更短的出块时间，比特币区块链只需要处理这些不同高速支付网络之间的比特币转移。这使得比特币可以按照人们的需求扩展，而不需要剧烈地增加区块大小。

竞争币（Altcoin）采用的是为一种新的特性创建一种新的密码学货币的做法，这使得外界认为密码学货币太混乱。竞争币似乎没有停止点，每一次分叉后还能继续分叉，无穷无尽，这造成了市场和开发的碎片化。他们认为，为了取得密码学货币的成功，必须建立网络效应，消除碎片化。他们也相信每个人应该享有无须向他们或者任何人寻求许可，进行自由创新的权利。他们需要一种不同的方式实现这个目标，而不是毁掉自己已有的成功。

为了实现这一点，他们提出了一种不需要另外创建新的密码学货币就可以创建密码学网络的技术。为实现这一愿景，他们需要继续投资比特币生态系统，和比特币生态系统进行合作，同时还需要得到许多知识渊博且具有专业背景的人的支持。他们感到在比特币生态系统和全世界范围内，缺少致力于创建无须信任密码学架构的公司。这就是他们和与其持有相同愿景的其他合作者走到一起建立Blockstream的原因。

Blockstream在未来也许也会开发一些侧链，但是侧链是一个开放的理念，任何人都能够（和应该）使用、开发他们想要的任何侧链。侧链

非常灵活，各种经济和技术试验都能在上面实施。如果开发者打算将一个现存的竞争链变成一个侧链或者与侧链相兼容的竞争链，它需要向比特币进行软分叉（softfork）或者联合锚定（federated pegging）。然后，它们能否成为侧链，取决于其是否接受竞争链的资产转到或者转出自己的区块链。如果现在的竞争链也想接受其他资产（例如比特币），与它自身的原生的竞争币平行，实现这一点的最简单办法是进行硬分叉。

他们认为在建立和支持基础架构方面具有巨大的商业潜力。例如为其他商业公司提供技术和服务，帮助他们转变到类似于比特币的做生意方式。现在他们的关注点是创建基础架构，从而在上面建立能够盈利的商业，再将获得资金投入建立更好的技术上。

据该公司介绍，区块链创业公司DAH已经决定使用Blockstream技术，以此作为超级账本的一部分。

Blockstream的核心创新是侧链，侧链是一种关注提高区块链的技术，分布式信任系统最强大的公用设施，能够与其他侧链和比特币区块链互相操作的区块链，避免了流动不足、市场波动、碎片化、安全漏洞和与其他密码学货币相关的欺诈行为。

比特币的交易存储在一个透明的被称为区块链的账本中。它由一个强大的分布式哈希网络来保证其安全性。侧链是一个确认来自其他区块链数据的区块链，使得比特币和其他资产能够在区块链之间进行转移，形成一个新的、开放的创新和开发平台。双向锚定使得比特币或者其他资产以一个固定的或者确定的汇率在区块链之间进行转移。一个锚定的侧链资产可以导入到其他侧链中，也可以从其他侧链转移回来。

侧链能够加强区块链的功能和隐私保护。它们的新扩展能够支持无数种资产类型，例如股票、债券、金融衍生品、真实和虚拟世界的货币，还能够增加像智能合约、安全处理机制和真实世界财产注册。

侧链还可以用于其他事情上，例如小微支付。它们允许试验和未来侧链的试验版本，甚至是一个测试版的比特币。

（二）Chain

金融领域的一些大鳄公司，已经投资了一家旧金山区块链初创公司Chain，涉及融资金额达到了3000万美元。投资方包括Visa公司、纳斯达克、花旗风投、RRE Ventures、第一资本金融公司、Fiserv公司、Orange SA等金融巨头。Chain首席执行官亚当·卢德威（Adam Ludwin）表示，智能的区块链网络能够从根本上改善资产的移动，很高兴能够与这些机构进行合作，也相信各方能够充分利用这场即将到来的、不可避免的市场格局变动。

这些支持Chain公司的投资方，还承诺共同成立一个“区块链工作组”，以促进对区块链应用持续和定期的讨论。该工作组预计每年举行两次会议。此外，该公司还表示，RRE Ventures首席执行官吉姆·罗宾孙（Jim Robinson）将加入公司的董事会，而卢德威也将担任RRE的负责人。

Chain.com正在帮助促进开发一个全新的媒介，并将现存的大部分的金融工具（美元、欧元、股票、债券、信用积分、通话时长）转换到这个媒介上面。这些资产已经是经济中不可或缺的一部分，但是在移动和储存的时候很不方便。卢德威认为，将世界上的资产数字化是一个巨大的市场，远大于增强或支持其中一种被称为比特币的资产。他宁愿在一个产值几兆亿而不是几十亿的市场里面进行。而且他认为Chain比现在做的任何事情都能更直接、更快速地影响人们的生活。

Chain.com即纳斯达克第一个主要的区块链战略部署的合伙人，并且帮助纳斯达克开发了Linq系统，是纳斯达克为私人股权市场搭建的新

平台，用来跟踪私有企业股权的转移。由于传统方式需要纸面记录，这一部分很长一段时间以来充斥着无效率。Linq于2015年12月记录了第一单交易，一个私人股权市场的会员在Chain.com上发行股票后，被一个使用区块链技术的投资者买下，缩短了结算时间，消除了纸质股权证明的需求。像Linq这样的解决方案，本质上属于一种市场分隔，既有足够的价值来证明其实用性，同时技术上已经足够成熟将其实现，也许将会在未来取得成功。

Chain.com也在为电信业、保险业和支付业做另外的企业项目。在电信业的一些应用包括协助电信企业介入金融服务，帮助他们协调漫游（一个用户不在所属服务器范围内通过其他服务器打电话或发短信时产生的）费用的支付（Chain.com的投资方包括一家电信企业Orange的投资）。在保险行业，主要是应用区块链技术于再保险市场（保险人出让一部分收益将风险转移给其他主体的市场）。

卢德威把2015年描述成以科技和企业的形式把这一项目推向市场的一年，他觉得这一年中有许多关于市场结构以及谁要第一个行动，谁将会从网络效应中得到最大收益的问题，这些在起步阶段都是不可避免的。他还预估近期Chain.com将会帮助7~10个项目启动，而且没有减缓的迹象。如果有的话，该项目会得到更多的行政支持、更多的资金、更多的绿灯。因为任何已有的网络都将会有很多机构来参与，大多数情况下每个网络都会有一个主要的发起机构以及一系列的参与者，这是一个非常现实的可能性，只有极少数的有意义的区块链网络最终进入市场并获得网络效应，但在这些网络上有很多的参与者，并且可能会有50家银行。毕竟，在这一领域的企业比专营比特币的公司有更大的优势。虽然比特币是数字货币领域应用最广泛的，但是它的流行程度远不及那些金融机构，比如Visa和Citi，而这两者都是Uphold的合作伙伴。

（三）Gem

Gem公司成立于2014年，其目标是开发基于比特币区块链的API产品。在早期为比特币开发者推出了多重签名API，并且会逐渐扩大API开发，为区块链应用开发一个模块化平台，进而应用到多个行业。

但是从2015年开始，Gem宣传其服务为提供不特定“区块链”的API，此举与其他如ChangeTip和Uphold等区块链公司一致，他们都在最近几个月里寻找在数字货币中将产品多样化的方法，而不仅仅局限于比特币，或者比特币区块链。

Gem公司的首席执行官麦克·温克尔施佩希特（Micah Winkelspecht）承认，最新的一轮融资发生在这家已成立两年的公司经营策略发生变化期间。他说，Gem公司的产品已经变得不再那么“集中于比特币”，因为公司正努力进入一种成长中的新型市场，主要在金融企业中研究区块链项目开发的专业知识。

温克尔施佩希特把公司的新模式与竞争对手区块链API提供商Chain进行比较。Chain不再专注于比特币后，在2015年9月的A轮融资中筹集到3000万美元。温克尔施佩希特依然坚信比特币是一种货币，但重点在于企业的使用实例以及与这些类型的公司一起探索相关产品，这才是Gem关注的焦点。

温克尔施佩希特表示初创公司“总能认识到”他们的产品需要与不同的区块链整合，并举出Gem结合litecoin和dogecoin区块链的例子。总的来说，截至2016年4月，Gem公司在三轮公开融资中已筹集到1040万美元。在最新一轮的融资中也看到了不少之前参与Chain 9月融资的公司，包括数字货币集团和RRE Ventures公司。

即使Chain已经减少了比特币API服务，温克尔施佩希特也表示Gem并没有计划停止支持与比特币相关的合作伙伴，比如Bitwage和Purse。温克尔施佩希特将这次的重点转移当成一种明智的决策，他认为，比特币行业的用户并不需要接受比特币基于产品和技术方面的教育。

他声明这点与新用户们的想法有很大的不同，新用户们经常要求更多的时间来学习如何利用技术满足他们的需求。**Gem**的目标不是成为一家咨询公司，做咨询的主要原因是客户需要帮助。帮助客户建立一个解决方案并顺利实践，需要消耗大量的时间。有了融资资金，**Gem**表示公司将寻求增加新的员工来补充现有的工程人员，这意味着将会增加相应的商业支持。

Gem新策略的核心在于他们相信比特币区块链不能满足企业客户的需求，因为它们不能让一些特定的使用案例满意。**Gem**还谨慎地表达出，当比特币工作证明式的挖矿网络和开放的共有算法成为这种分布式全球货币的重要组成部分时，他们可能会限制该技术的广泛应用。

坦率地说，金融机构并不需要能抵制审查的区块链，他们倒是很需要快速的以及能代表传统资产的产品。因此，**Gem**相信未来将会有许多可用的区块链，有些将侧重于解决智能合同和自动化，有些将侧重于面向金融的交易，还有些将侧重数据管理。在将来，肯定会出现公有的链和私有的链，且它们都会取得成功。

八、物联网和供应链

Filament是一个雄心勃勃的项目，通过使用小型且先进的硬件设备把各种电子设备，特别是电器放在区块链上来建立物联网。Filament能够让你在不必成为安全方面、可扩展方面或者网络堆栈方面的专家的情况下，建立一个可链接的模式，即在一个工厂铺满传感器或者是控制整个城市的路灯——Filament的独立网络可以跨越数公里并且维持数年而不需要WIFI（无线网络）或者蜂窝网络。

在2015年8月，Filament宣布完成了500万美元的A轮融资，投资方是Bullpen Capital、Verizon风投和三星风投。

这是电子消费产品巨头三星的下属投资部门三星风投第一次参与投资区块链行业。之前，三星风投因参与IBM的ADEPT项目而轰动一时。ADEPT项目是利用比特币和以太坊网络打造的去中心化的物联网，IBM与三星选择了三种协议：BitTorrent（文件分享）、以太坊（智能合约）和TeleHash（P2P信息发送系统），利用这三个协议来支撑ADEPT系统。

Filament的联合创始人兼首席执行官艾瑞克·杰宁斯（Eric Jennings）认为，Filament是一个使用比特币区块链的去中心化的物联网软件堆栈，能够使公共分类总账上的设备持有独特身份。通过创建一个智能设备目录，Filament的物联网设备可以进行安全沟通、执行智能合约以及发送小额交易。

Filament与ADEPT项目在本质上是相似的，不同的是它将针对工业市场，使石油、天然气、制造业和农业等行业的大公司实现效率上的新突破。许多公司在建立网状网络或区块链方面缺乏经验，但他们清楚自己需要连接这些网络以提高效率。而Filament就可以为他们提供这样的

解决方案。

Filament将开发两个硬件设备：FilamentTap，一个传感器装置，允许装置与周边10英里^[1]以内的电话、平板电脑和计算机进行沟通；FilamentPatch，用来扩展该技术的硬件，可以实现硬件项目的定制。

Filament表示，通过利用基于区块链技术的堆栈，企业可以更好地管理物理采矿作业或农业灌溉，而不需要再使用效率低下的中心化云方案或文件式的老方案。

Filament成立于2012年，公司原先的设想是建立网状网络上的无线家庭安全系统，后更名为Pinocc.io。2014年10月，该公司的项目被选入了TechStars孵化器，于是又更名为Filament，并把公司的发展目标定位在工业用例上，实现设备之间的连接。

Crosslink Capital、数字货币集团、Haystack、Working Lab Capital和TechStars也参与了Filament的A轮融资。在资金的帮助下，Filament表示会扩大公司团队，从15人扩大到30人，并且在2015年第四季度推出硬件设备。

^[1]1英里≈1.61千米。——编者注

九、智能合约

（一）Augur

1.什么是Augur

Augur是建立在以太坊平台上的去中心化预测市场平台。利用Augur，任何人都可以为自己感兴趣的主体（比如美国大选谁会获胜）创建一个预测市场，并提供初始流动性，这是一个去中心化的过程。作为回报，该市场的创建者将从市场获得一半的交易费用。普通用户可以根据自己的信息和判断在Augur上预测、买卖事件的股票，例如美国总统大选。当事件发生以后，如果你预测正确、持有正确结果的股票，每股你将获得1美元，从而你的收益是1美元减去当初的买入成本。如果你预测错误、持有错误结果的股票，将不会获得奖励，从而你的亏损就是当初的买入成本。

许多因素使得Augur不同于传统的预测市场，但最重要的区别是，Augur是全球化与去中心化的。世界各地的任何人都可以使用Augur，这将为Augur带来空前的流动性、交易量和传统的交易所不曾有过的多种视角和话题。

Augur系统内部使用一种名为信誉（REP）的代币。REP可以被看作一种与个人的公、私地址相关的“积分”，像比特币一样可分割和可交易。然而，只有这点属性类似于密码学货币。如果说比特币模拟黄金，那么REP则是模拟信誉。

Augur的去中心化还体现在事件结果报告机制上。在传统的中心化预测市场，当事件发生后，由中心化的人或者组织确定事件结果。与此

不同的是，Augur采用去中心化的事件结果报告机制，从而引入REP代币。当事件发生以后，众多REP持有者对事件结果进行报告。同时，普通用户无须持有REP即可在Augur上进行预测、交易。

持有REP的人被期望每8个星期对系统中随机选择的到期事件 / 预测的结果进行报告。持有者只需要三个选项：是的（事件发生了）、不是（事件没有发生）、模糊不清 / 不道德的（如果持有者认为结果模糊不清，可以将报告推迟到下一期，在最终没有决议就结束事件以前），报告者有两个星期的时间来做报告。当然大家都期望这一过程能够十分快速地进行，当Augur普及以后，这一过程将可能在一小时内完成。

如果信誉持有者在两个星期的投票期内没有报告指派给他们事件的结果，或者进行不诚实的报告，主成分分析法（PCA）会把懒惰的、不诚实的持有者的信誉重新分配给经常报告和诚实报告的持有者。只有诚实的信誉持有者将从每一投票过程中获得交易费用。

2.全体预测市场的准确性

（1）糖豆案例

在2007年，哥伦比亚商学院教授米歇尔·毛布森（Michael Mauboussin）让他的73位学生估算瓶子中糖豆的数量。学生所估计的数量在250~4100个。其实瓶子中有1116个糖豆，学生们估计值与真实值1116之间平均偏离700，也就是62%的错误率。然而，尽管学生的估计很不准确，但是他们估计的平均值是1151，与真实数值1116只有3%的误差。

这一研究以各种形式被重复过多次，结果都与上面相同。Augur正在将这种群体智慧应用到每一个学科中，从政治学到气候学，并用利益得失来强迫群体说真话。

（2）潜艇案例

在1968年5月，美国的一艘名为Scorpion的潜艇，在大西洋完成执勤任务后返回纽波特纽斯港口的途中消失了。虽然海军知道潜艇最后的报告位置，但是不知道Scorpion发生了些什么事情，只知道最后一次联系后潜艇大致的前行方向。最后他们将搜索范围确定在方圆20英里，几千英尺深的区域^[1]。这是一个希望渺茫的搜索。人们能够想到的唯一可能的解决方案是，召集三四位潜艇和洋流的顶级专家，让他们判定潜艇在哪里。但是，根据谢里·桑塔格和克里斯托弗·德鲁（Sherry Sontag and Christopher Drew）在《盲人的骗局》（Blind Man's Bluff）中的记录，一位名叫约翰·克雷文（John Craven）的海军军官提出了一个不同的计划。

首先，克雷文设想了一系列可以解释Scorpion可能发生事故的情景。然后，他召集了一组具有不同背景的人，包括数学家、潜艇专家和搜救人员。克雷文让他们猜测哪种情景的可能性最大，而不是让他们彼此商量得出答案。为了让猜测更加有趣，克雷文采用了下注的模式，奖品是芝华士（Chivas Regal）酒，参与的成员就潜艇出事故的原因、下沉的速度、倾斜的角度等问题进行打赌。

没有一段信息碎片能够告诉克雷文潜艇在哪里。但是，克雷文相信，如果他将小组成员提出的所有答案汇集在一起，针对潜艇沉没做一个完整描述，他就能够知道潜艇在哪里。这就是克雷文所做的事情。他利用了所有的猜测，使用被称为“贝叶斯理论”（贝叶斯理论是计算事件的新信息如何改变你对此事件原有预期的方式）的公式，判断潜艇的最后位置。做完这些事情后，克雷文获得了团队关于潜艇位置的集体估计。

克雷文得出的位置并不是团队任何单个成员所猜测的位置。换句话说，团队中每个成员的猜测与克雷文使用汇集起来的所有信息得出的位

置一致。最后的判断是一个由团队整体做出的集体判断，而不是代表团队中最聪明的人的个人判断。这是一个绝妙的判断。

Scorpion潜艇失踪5个月以后，一艘海军船发现了它。潜艇被发现的位置与克雷文团队猜测的位置仅相差约200米。

这个实例的惊人之处在于，这个团队几乎没有任何可信赖的证据，只是一些数据碎片。也没有人知道潜艇为什么沉没，没人知道潜艇下沉的速度和倾斜角度。虽然团队中没人知道这些信息，但是作为一个整体的团队却可以知道这些信息。

（二）Symbiont

1.项目介绍

Symbiont成立于2015年初，公司创始人曾经创立过基于比特币协议的合约币（Counterparty），创始人有：罗比·德莫迪（Robbie Dermody，总裁）、伊万·瓦格纳（Evan Wagner）、亚当·克雷伦斯坦（Adam Krellenstein，首席技术总监），以及MathMoney（fx）的创始人马克·史密斯（Mark Smith）。Symbiont正在建立首个用于发行区块链智能证券（Smart Securities）和交易智能证券的平台。

Symbiont的专有智能证券技术为复杂的金融工具提供了一个模块，从而使编程语言更容易理解，也使分布式总账全面数字化的过程更加简单。

如今市场所采用的人工手段很容易出错，而智能证券技术能够数字化流程并自动运作。与传统方法相比，这些“智能证券”是能够自我加强、自我执行的合同，大大降低了成本，提高了效率。由于Symbiont整合了硬件安全模块安全网（HSMs），监管高层对加密交易机构有了更

多的信任，允许这些机构操作交易。

Symbiont起源于Counterparty项目，这些创始人也分别是Overstock公司旗下Medici项目（现t0）的前成员。2015年3月，三人所创立的Counterparty与马克·史密斯的Money（fx）公司进行了合并。Counterparty是建立在比特币区块链之上，早期的数字货币2.0项目之一。在本质上，它可以允许用户执行不同的金融应用，而不仅仅是比特币的P2P支付网络，并且它也受到比特币网络的保护。

Counterparty是一个针对比特币区块链的非营利、开源社区驱动的项目软件套装和协议。与Counterparty的其他创始人罗比·德莫迪和伊万·瓦格纳一起，克雷伦斯坦创建了Symbiont，一个面向所有机构的软件提供商，交付智能合约的全套解决方案，马克·史密斯后来也加入进来。

区块链技术已经在金融界获得了广泛的关注，这种去中心化的公共总账，将可能改变这个行业记录或处理事务的方式。世界各地的一些银行，都在努力探索将区块链技术用于他们的内部运作中，而一些有远见的公司，例如Overstock，已经在尝试将比特币的相关技术用于证券清算。对Symbiont而言，区块链技术可以通过“智能证券”或“智能合约”来重塑华尔街的未来。

马克·史密斯表示，该公司计划专注于私募股权市场。现在许多创业公司都在避开公开发行的股票，而健壮的私募证券市场，可能会是金融的未来。例如Uber这样的公司，已经完成了K轮或者N轮融资，上市的诱惑力对他们而言，已经没有过去那么强烈，其实是可以转移到其他的证券上的。比如Symbiont可以证明，某家企业在比特币区块链上发行了债券，然后就可以在一个可管理的总账系统上进行了。

除了私募股权投资，Symbiont也看到了企业债券市场的潜力。Symbiont认为，区块链技术在银团贷款市场是有未来的，其中贷款方可以组团为借款方提供资金，从而分散违约的风险。克雷伦斯坦解释说，

Symbiont有一个智能证券系统，它建立在比特币之上，并且会对执行数据以及交易中公布的数据进行编码，然后发布到区块链上，因此，所有的数据都是在比特币区块链上的。

2.智能证券的重要性

其一，能够为任何金融工具类别的复杂机制、现状与互动建立模块。

其二，能够执行金融工具的整个生命周期，包括发行、初级市场配置以及二级市场交易。

其三，通过严格而强硬的访问规则，任何市场参与方都能够了解到工具的现状，并且访问其公司行为的界面。

其四，平台的情况及执行公司行为的电脑代码，都会以一种防篡改的形式公布在分布式总账上，使所有相关方都能看到。

[\[1\]](#)1英尺=0.3048米。——编者注

十、存储与下一代互联网

（一）Storj

2014年4月，开源、去中心化存储平台Storj，赢得了美国得克萨斯州比特币会议的黑客马拉松奖，获得了小蚁比特（BitAngles）基金25万美元投资。

云存储的未来是去中心化的。想象一下，你能够通过自动网络出租额外的硬盘空间，并获得密码学货币回报。由于中本聪的发明和例如Storj、MaidSafe、Ethereum这样的平台，这一切都能够实现。现在我们有能力将P2P货币与例如存储空间、带宽、CPU（中央处理器）算力连接起来，例如Dropbox和Google Drive（谷歌硬盘）这样的云存储服务就可以有自己的专属货币。

不同于其他比特币2.0平台，Storj决定以“小步走”的方式开发他们的软件。他们想首先开发小规模的系统，作为原型使用。因此他们开发了被称为Metadisk的拖放文件托管网页应用。需要注意的是Metadisk只是Storj平台的一部分，团队将会继续开发更多的网页应用，例如DriveShare（用来出租你的硬盘空间），最终形成一个更紧密结合的完整的去中心化存储平台。

（二）MaidSafe

MaidSafe是一家位于苏格兰特伦（Troon）的英国创业公司。该公司认为，当前互联网存在的问题可以追溯至互联网底层的架构设计。为

解决这些顽症，探索可持续的数字内容商业模式，保护用户数据和隐私，以及对抗黑客、恶意软件和过度监控，答案在于重新开始，设计全新的互联网架构。

MaidSafe从2006年以来就在开发自己的新网络，并于2014年早些时候结束了“保密模式”，开始展示其实用计划。当时，该公司正在部署3个测试网络之一，在不运行任何应用的情况下测试底层网络。该公司在2014年第四季度启动了完整的beta测试（一种验收测试）。最初的测试网络包括180个节点，分别位于新加坡、旧金山、阿姆斯特丹和纽约。

MaidSafe是一个完整的跨平台、去中心化的自治数据及通信网络。在实际应用中，即是一个无须中间服务器和数据中心的网络，完全基于点对点架构。因此，MaidSafe将Skype前首席运营官米歇尔·约翰逊（Michael Jackson）作为顾问，而Skype是P2P技术的先驱。

相对而言，这一网络的用户自身也是网络基础设施的一部分，需要贡献出一部分硬盘空间。这一网络构建了激励机制，当用户贡献硬盘空间时将向他们回馈名为“SafeCoin”的加密数字货币。因此，正如许多人为了获得比特币而进行挖矿活动一样，MaidSafe网络的用户在提供计算资源之后将可以获得SafeCoin作为补偿。MaidSafe也希望，随着网络规模的扩大，SafeCoin的价值也将水涨船高。

MaidSafe能将网络内的所有计算机联系在一起，形成类似巨型计算机的设备，或者称为“巨型数字大脑”。因此，这一网络将所有节点联系在一起，在不需要实际数据中心的情况下，将这些节点变成巨大的数据中心。这是一种能取代数据中心，甚至可以取代大型科技公司的网络基础设施。这家创业公司还希望重新配置当前的互联网架构，弱化大型数据中心和平台所有者掌握的权力及中心地位，将权力重新还给个人用户。

个人开发者也将从中受益。在MaidSafe网络中开发应用的成本将低

于采用当前的主机模式，建设一家创业公司不需要支付任何主机成本。AWS（Amazon Web Service，亚马逊云服务）和Rackspace（全球三大云计算中心之一）将不再必要。在这样的网络上进行开发不需要任何前期费用，MaidSafe的API也是免费的。

MaidSafe网络的用户贡献出闲置的硬盘空间，将成为网络节点。随后，MaidSafe网络利用大量用户的空闲计算资源形成互联的存储服务，因此存储功能不会集中于某些专门的数据中心。网络无须任何中间人来提供数据。用户可以直接访问网络，而网络也可以直接访问用户的电脑。

MaidSafe是全球首个自主运行、不需要服务器的网络，并支持自我认证。如果某些节点离线导致数据丢失，那么网络能重新创建数据。MaidSafe网络同时也能够抵御病毒，无须服务器，目前没有其他网络能同时实现自治及无服务器。

在MaidSafe网络中，用户使用数字服务时不必暴露自己的隐私，而是只要付出目前并不使用的硬盘空间即可。相对于当前模式，这是一种更公平、更平等的“客户端/服务器”关系。与此同时，通过MaidSafe网络发送的数据在本地加密，随后通过软件进行分块，并经由未知节点随机发送。因此，所有数据以大规模去中心化的方式来存储，能抵御黑客攻击和窃听。

通过服务器和数据中心对数据进行集中存储将带来问题，即数据非常容易受到攻击。这些数据很容易被黑客窃取，无论是由于公司追踪活动还是政府监控，甚至一些政府还会尝试控制用户能访问的内容。因此，基于中间人的方式应当被舍弃。

（三）Sia

1.项目介绍

Sia最初的设计目的是：让云储存去中心化。当前，大多数数据由一个中心如AWS托管。一个单一的企业掌握着所有的数据，而且数据常常是不加密的。当前，把数据放在云中需要信任，即必须相信亚马逊会保存你的数据并尊重你的隐私权。而Sia准备建立一套完全不同的系统来把数据放在云中。即提供一个去中心化的、有奖励机制的、可抗拒拜占庭错误（byzantine fault-tolerant）的云储存系统，而这个系统将与类似的中心化系统（主要是像支持Dropbox的AWS S3这样的系统）产生竞争。

使用Sia时，数据被存在多个存储供应者的主机里。Sia的设置是可以调整的，但系统的标准设置是把一个文件存在30个托管主机里。一种称为Reed-Solomon代码算法使Sia可以把一个文件分成多个部分，并把每个部分分别存于各个托管主机里，这样一来，只要10个托管主机就足够恢复一个文件。这个10对30的方案意味着文件会有三个备份。假设每个托管主机的可靠性是90%，那么这个文件本身的可靠性将达到99.999999999%。即使托管主机没有非常好的在线状态，文件却有相当好的在线状态，可以在多个地区间选择托管主机的能力意味着Sia不受地区网络瘫痪的影响。

所有用户数据在进入Sia客户端的时候都被分割成很多小块，只留下用户恢复原始数据的少数片段。敏感用户信息块被压缩到4MB，用于保护用户隐私。最后，每个压缩块又使用客户端的密钥进行加密。主机接收到一个加密的二进制块，并且没有关于文件其他部分的信息。即便是黑客们发现了，他们也仍然需要破解众多的加密密钥用以恢复文件。客户保存有加密校验，如果主机试图篡改数据，它将提醒用户注意。

Sia平台严格而复杂的加密和去中心化分布式文件系统可被用于去中心化应用开发。它的API使得开发者可以直接在Sia客户端存储文件，

允许第三方应用用户直接访问他们的客户端数据存储系统，并且不需要改变原来的客户端。

每一个托管主机都受到加密文件合约的约束。当一个文件上传时，同时形成的合约将确保托管主机只有在完成了预定的时间段里保管文件的条件后才能拿到支付款。托管主机也需要提交一定的押金，如果一个托管主机没有完成合约，它不仅得不到支付款，而且还会失去押金。在文件上传时，上传者清楚这个系统有很强的抗虚假托管主机，以及这些虚假托管主机会受到很严重的金钱惩罚。区块链让这种合约成为可能。

第三方应用和Sia平台用户都有权发布在文件存储上的智能合约。这种特性就使得上传者和主机在存储要素上达成共识，包括存储期限、付费计划和总额，并且可以将信息嵌入到区块链中，自动建立一个不可更改的合约。当合约到期时，主机就会提交一个存储证明至区块链，显示它仍然是合约定义的文件。如果证明是有效的，上传人员的钱将被支付到主机，主机将返回抵押品。但是如果主机提交了无效的证明，或者没有提交证明，那么所有的钱都将还给上传者。

2.应用场景

Sia最大的优势之一是为云储存引进了一种自由市场机制。今天，要成为一个云储存提供者意味着要建立品牌、建立信誉，配以客户服务和支持系统，并且往往需要建立一整套生态系统。Sia消除了所有这些成本消耗。如果你有一个硬盘和互联网连接，你只需要把你的电脑与Sia平台接通就可以开始接受云储存合约和业务。其他人不需要知道你是谁或信任你，你也不需要宣传自己和处理客户服务事项。这有些像比特币的挖矿，你只需要简单地接通电脑，就可以开始挣钱。有便宜资源的人们可以通过向世界各地提供廉价的云储存来谋取巨额利润。在Sia系统里，没有一成不变的供应商和隐私规则（因为在Sia中隐私是彻底的和自动的），只有一种纯粹为储存和宽带而建的自由市场。我们相信

这会导致现有市场价格的急剧下降。在测试平台里，我们已经可以看到储存的费用非常低（以现在测试平台中的价格计算，即使使用标准的8倍备份，它的价格也只是传统云储存价格的3%）。

文件内容的分销商（如Netflix、Spotify，或YouTube）能够通过使用Sia的内容分销网而获益。当前的文件内容分销网成本高而且有大量的重复，并且在许多服务器上运行，且这些服务器都是由单一中心来控制的。Sia则能够给互不信任的托管节点付费并使用加密合约来强制执行市场供求协议，这样一来，Sia可以把云储存业务外包给这些托管节点。在使用Sia的时候，文件内容的分销网已经被内置于Sia之中。它还可以为有争议的业务提供一定的保护。比如，Comcast试图遏制Netflix的流量运行。在Sia中，所有流量运行都相同，Comcast将很难筛选并遏制某些流量运行。Sia的自由市场模式也将意味着对于宽带密集型的服务业务来说，分销成本可能有实质性的下降，因为便宜的节点将被优先选用，这也意味着高价的托管节点将可能根本得不到业务（从而增加了降价的压力）。

未来超高速的互联网还会带来一些有趣的可能性。一个超高速的互联网的连接将和固态硬盘连接一样快。使用Google光纤或类似的产品，你的电脑可以不使用硬盘，而可以直接从网上下载所有的东西且其速度和使用硬盘一样快。你将可以把整个电脑上的软件都储存在Sia上，根本就不再需要其他诸如硬盘类的储存方式，并能达到同样的效果。这意味着你可以在世界任何一个角落启动和运行你的个人运行系统和设置，而无须使用任何硬盘设备，如USB（通用串行总线）和CD（光盘），你只需一个简单的互联网连接即可。这种情况一般不会发生在传统的运行系统里，由于其极端的滞后性，如果你能设置一个内存磁盘运行系统（即整个运行系统在一个内存上），并时不时地让它和云储存服务同步，这样速度就不会因为没使用硬盘而受到影响。

比特币的潜在前景之一是把广告从互联网上消除，并用一种付费墙

取而代之。比特币可以使这种付费墙设施比任何现有的付费墙都更简单方便。它能使一个用户只需付零点几分钱就可以浏览一个需付费浏览的（但没有广告）网站一定的时间，但这个用户可能再也不会浏览这个网站。如果使用比特币，这种情况可以以一种去中心化的形式来完成，但如果这个网站和这个用户不需要在同一家付费服务公司里，他们只需要在同一个去中心化的付费网络中即可。启动这种服务只需要相当短的时间。然而这里有一个很大的问题，即从免费服务到收费服务的转移。即使它已经消除了广告，但它需要你真的花钱，这会造成巨大的心理障碍，即使这种费用每月不过几分钱。从心理上讲，人们也不喜欢付大量的微小额度款项。

在Sia生态系统中，从一开始，这种付费模式就被强制使用。在这个去中心化的系统里没有免费储存，也没有免费的5GB（千兆）试用，无论它多么便宜。小额度的免费使用和Sia这种机制不相称。Sia上的储存和使用是仪表计量付费制。值得庆幸的是，在我们今天的社会生活里有许多成功的仪表计量付费的例子。第一种重要的例子是先用后付的模式。你的公用事业公司就使用这种模式。当你打开电灯时，当你洗澡时，当你使用洗碗机时，你的公用事业公司实际上在向你处收取一些少量费用。在一个月的使用过程中，这些小额费用会积累成一笔可观的费用，但是你已经习惯了这种方式，而且总体上你大致清楚在什么情况下账单会比较贵。而你在月底会乐意付水电费。第二种模式是先付后用。给汽车加油就是一个不错的例子。每次当你开车时，你会意识到你会消耗汽油而且不久就需要加些油，而且加油时你得一次性付清油费。但你依然乐意开车，因为你知道这是物有所值。

在以上两个例子里，关键是你并没有边使用边付费，而是隔一段时间付一次费。你知道每当你使用时你都在花钱，但你只需在月底付一次钱。当缺钱的时候，你会限制你的消费以免账单费用过高。这些模式很适应人们的心理条件。Sia选择了加油的模式来计算消费。当你开始使用Sia的时候，你得先在你的账上充值（相当于加油），而且你能知道

充值后大概可以用多久。当你账上的钱快用完的时候，你会得到一个“低油量”的警告提示你需要再次加油了。由于Sia有内置的付费通道，从未知的服务器和单位下载资料不需要设置任何的时间。只要上传者 and 储存主机维护者双方均在同一个全球性支付网络中（这个网络由许多相互并不信任的单位组成），他们相互之间可以进行及时且安全的钱款转移。这种付费网络可以有利于上传和下载。

它还完全可以使网上浏览的体验变得更加美好。Sia的付费网络并不只限于去中心化的储存业务，而且内容和资料并不需要直接从Sia的去中心化网络里下载。在使用Sia时，你可以访问和管理中心化网站中的付费墙，以便消除广告并且能够给网站维护者带来更多的收入来源。

目前，Sia的核心焦点是去中心化云储存系统，更具体地说，它就是一种去中心化的对象（objects）商店。在这个平台上，你可以存放和领取各种各样的文件，并能上传只由一个散列组成的一个查询内容。上传简单，且保证文件安全简单，把文件在电脑间传递（如你和朋友之间）也十分简单。寻找你想要的文件也较为容易，而且最重要的是，绝对不会让用户担心上传的文件是否丢失。

Sia也发布了与Crypti合作的消息，Crypti是灵活的后台应用开发平台。在这项合作中，Crypti的工程师可以集成Sia的API，访问Sia的数据存储客户端。作为Sia去中心化应用开发的存储层，Crypti已经集成了Sia。Sia提供了API，可以上传文件到存储网络。Crypti是一个灵活的平台，可以集成多个后台，但是Sia是第一个去中心的尝试，允许开发人员创建实实在在的非信任Crypti应用。

最开始的Sia设计针对安全性、隐私权和数据的完整性。然而在建立这个网络的过程中，Sia也建立了一个开放的市场，在这里任何托管主机都可以参加，并且纯粹以商业信誉来论好坏。一个托管主机的等级将取决于它的速度、价格和可靠性。托管主机将无须考虑客户服务、品牌建立或法律条约等成本花费，托管主机只需在一个层面竞争：在技术

上谁更好。其结果将是一个高度竞争的、价格不断趋于下降的、更加可靠的和不断提速的网络。Sia的目标不仅仅是最安全的云储存平台，而且还是最快的和最便宜的平台。在早期，可以看到Sia的价格只占传统云储存平台的10%~20%。目前，Sia云存储网络售价是每TB（百万兆）每月3美元。据网站所述，该网络上已经存储有超过1TB的数据。

Sia网络的超级并行性意味着上传和下载速度可以满足绝大部分连接要求。大型分布式节点阵列意味着Sia是一个强大的CDN（内容分发网络）。广义网上不存在编程逻辑，使得Sia在面对电力中断方面更具灵活性，比如在电力供应中断和发生自然灾害的时候。Sia网络在具体实现上的各方面都是非常先进的。

总之，Sia是一个基础设施，它为所有需要远程储存的应用软件打下基础。类似于去中心化的存储项目Filecoin和Storj，Sia的目标是建立一个非信任的、具有容错能力的文件存储服务。无论你是备份你的计算机，传输你的影视文件，还是同步几个机器间的文件，Sia所建立的这个基础设施在将来可以确保数据的安全。

（四）IPFS

IPFS（The Inter Planetary File System）是一种点到点的分布式文件系统，它连接的计算设备都拥有相同的文件管理模式。从某种意义上来说这个概念跟Web的最初理念很类似，但是实际上IPFS更像是互相转发Git目标的单个BitTorrent用户群。IPFS具备成为internet子系统的素质，通过合理配置可以完备甚至替代HTTP（超文本传输协议）。这听起来已经有些不可思议，但其实它可以做到更多。

IPFS的开发目前处于alpha试验阶段，还没能替代现存的网站存储系统。就像其他复杂的新技术一样，有许多地方需要进行改进。但IPFS不

是空想，它一直在实际运行着，任何人都可以试着在自己的电脑上配置IPFS，为访问用户提供服务。尽管IPFS的开发还不十分成熟，但有人认为在未来，IPFS将会取代HTTP。

IPFS从根本上改变了HTTP查找的方式，这是它最重要的特征。使用HTTP查找的是位置，而使用IPFS查找的是内容。例如，服务器上运行着一个文件`https://neocities.org/img/neocitieslogo.svg`，遵照HTTP协议浏览器首先会查找服务器的位置（IP地址），随后向服务器索要文件的路径。这种体系下文件的位置取决于服务器管理者，而用户只能寄希望于文件没有被移动，并且服务器没有关闭。

IPFS的做法则是不再关心中心服务器的位置，也不考虑文件的名字和路径，只关注文件中可能出现的内容。把`neocitieslogo.svg`文件放到IPFS节点，它会得到一个新名字：

QmXGTaGWTT1uUtfSb2sBAvArMEVLK4rQEcg5bv7wwdzw

这是一个由文件内容计算出的加密哈希值。哈希值直接反映文件的内容，哪怕只修改1比特，哈希值也会完全不同。当IPFS被请求一个文件哈希时，它会使用一个分布式哈希表找到文件所在的节点，取回文件并验证文件数据。

IPFS是通用目的的基础架构，基本没有存储上的限制。大文件会被切分成小的分块，下载的时候可以从多个服务器同时获取。IPFS的网络是不固定的、细粒度的、分布式的网络，可以很好地适应CDN的要求。这样的设计可以很好地共享各类数据，包括图像、视频流、分布式数据库、整个操作系统、模块链、8英寸软盘的备份，还有最重要的——静态网站。

IPFS文件还可以抽象成特殊的IPFS目录，从而标注一个可读的文件名（透明的映射到IPFS哈希），在访问的时候会像HTTP一样获取一个

目录索引。在IPFS上建立网站的流程和过去一样，而且把网站加入到IPFS节点的指令只需要一条：`ipfs add-r yoursitedirectory`。网页间的连接不再需要人去维护，IPFS自带的查找可以解决。

IPFS不会要求每一个节点都存储所有的内容，节点的所有者可以自由选择想要维持的数据。就像书签一样，在备份了自己的网站之后，自愿为其他关注的内容提供服务，所不同的是，这个书签不会像以前一样最终失效。

IPFS节点间的拷贝、存储和网站支援都很容易，只需要使用一条指令以及网站的哈希，例如：

```
ipfs                                pin                                add-r
QmcKi2ae3uGb1kBg1yBpsuwoVqfmcByNdMiZ2pukxyLWD8
```

剩下的IPFS会搞定。如果IPFS得以普及，节点数达到一定规模，即使每个节点只存放一点点内容，所累计的空间、带宽和可靠性也远超HTTP能提供的。随之而来，分布式Web将会变成地球上最快、最可靠、最大的数据仓库，人类知识也就再也不会湮灭，亚历山大图书馆永远不会倒塌。

IPFS哈希只能用来表示不可变数据，因为一旦数据改变，哈希值也会改变。从某种意义上来说，这是保持数据持续性的最好设计。但是也需要一种方法来标记最新更新网站的哈希，这种方法称为IPNS。

IPFS哈希是网站通过哈希公钥生成的，相对的IPNS使用私钥来标记IPFS哈希的引用，像比特币地址就是一种公钥哈希。IPNS公钥指向的位置是可变的，公钥的值则是保持不变的。随着IPNS的引入，网站升级的问题可以顺利地得到解决。

由于IPFS/IPNS的哈希值都是很长和难记的字符串，所以IPFS兼容

了现存的域名系统（DNS），即可以通过可读的链接访问IPFS/IPNS内容。其使用方法是在nameserver上创建一个文本记录，插入网站的哈希值。

IPFS还计划支持Namecoin。Namecoin从理论上完全实现分布式Web的去中心化，整体的运行中不再需要中心化的授权。支持Namecoin的IPFS不再需要ICANN、中心服务器，不受政治干涉，也无须授权证书。这听起来难以置信，但却是今天可以实现的技术。

IPFS在实现上加装了HTTP网关，使现有的浏览器也可以访问IPFS。因此无须等待，现在就可以开始使用IPFS作为存储、分布和搭建网站的设施。

十一、其他领域

（一）Maker

DAI Bond（Decentralized Autonomous Insured Bond）是基于以太坊技术的一种可转让的、彼此等价可互换的“加密债券”，本质上它试图在不稳定的数字货币上构建出稳定的数字货币，原理是通过一部分人来吸收其中的不稳定性从而释放出稳定的数字资产。如果能够成功，将在区块链世界中诞生稳定的数字货币来大规模使用。

Maker公司的创始人符文·克里斯坦森（Rune Christensen）分享了区块链技术在银行业的应用，如把数字货币的短期稳定性和区块链的长期稳定性结合起来的一家去中心化银行。他们相信区块链技术可以通过财务透明保证市场稳定。

DAI Bond从设计上就保证了参与者在彼此不信任的情况下也能够正常运行，参与者既无须事先认证，借贷行为也是低风险的。贷券的发行人（借款方）通过在以太坊区块链上锁定比特币、以太币和其他加密数字资产作为抵押品来发行贷券，然后再把这些贷券在市场上卖给贷券持有人（出借方）以换回流动性好的资产/货币。贷券的持有人之所以买入贷券是为了赚取稳定的现金流，这部分现金流来自借款方抵押贷款所需支付的利息。而“做市行”（Maker）作为一个“去中心化自治组织”，为此系统的每一个用户提供有限的违约担保，并收取保费作为回报。

（二）Bitwage

1.项目介绍

就用户数量而言，Bitwage是业内最大的比特币工薪支付服务提供商。Bitwage提供的三种主要类型，即个体工资、雇主薪资和国际薪资，使用户发放以及接收比特币形式的工资变得极其简单。使用比特币发放工资有以下两个好处：对于雇员而言，这种方式可靠便捷，取款不需要银行；对于雇主而言，有助于获得和留住高质量的人才，解决支付外国员工不方便的难题，而且能节省时间和花销。

不管他们的雇主是否签约Bitwage，个体工资都能为任何员工提供以比特币形式发放工资的服务。雇主薪资能让雇主享受到以比特币发放工资的益处。国际薪资使公司能为来自世界各地的员工提供比特币形式的工资发放服务，同时为雇主、雇员和自由职业者节省90%以上的国际支付手续费，从而使得在整个薪资支付过程中，客户们感觉就像是在使用当地货币般舒适。跨国工薪发放的平均手续费是8%，正常情况下5个工作日内资金会到位，而且没有外人知道资金的去向。

Bitwage正在构建国际收支的未来，这是创造力与时间观相结合的产物。通过区块链技术来为客户实现跨国资金转移，取代了老式的通过数个中介机构转移资金的方式，从而避免了被数次收取手续费、交易进度耽搁和资金遗失的风险。因为没有中间商的介入，客户可以随时了解资金的动向。Bitwage使用了区块链这项神奇的技术，并在客户使用其在银行之间、云储蓄和借记卡转出和接收资金期间，让客户们享受到无尽的好处。

由于整个过程都涉及资金流动，我们可以看一下阿根廷的例子。考虑到他们当前金融系统的运行方式，在阿根廷运行这种支付方式，需要顾客缴纳交易额30%~40%的交易手续费。这主要是因为官方汇率和实际汇率有较大的出入。非阿根廷国籍的人以美元兑换阿根廷币时必须或多或少地经过国家的限制，而且要以官方汇率兑换。

然而，阿根廷政府不把比特币视为货币。这意味着你可以将比特币转给别人，收款人随后可以将比特币从美国“携带”至阿根廷，然后在本地的交易所按当地的汇率兑换。所以，在这个案例中，直接将美元转至阿根廷币是不合法的，但使用比特币来发放工资却是合法的，同时也方便了员工在阿根廷当地的交易所兑换比特币。

目前，一些自由职业者协同Bitwage的云储蓄技术在进行这个项目，它能使你的资金以20多种不同的货币和贵金属的形式储存，包括美元和黄金，然后根据个人需要，以阿根廷币的形式从账户中支出比特币。

不管是大人物还是小人物，比特币支持者还是反对者，Bitwage都将让他们接受用比特币支付工资。如果雇主把工资直接打到工资本上，只需要切换一下账户，就可轻松实现比特币转换。

Bitwage用户可以任意比例转换，可以是100%也可以是1%，完全自由。Bitwage发现，在支持比特币的公司中，47%的受访者对比特币工资持欢迎态度。2015年5月，Bitwage对150家支持比特币的公司进行了一次社会调查，这些公司主要在美国。其中38家受访公司积极响应，18家公司即将使用比特币支付工人工资，10%的公司早已使用。其他受访公司就未使用比特币工资做出了详尽的解释，其中18%的公司表示未来会使用，16%的公司渴望使用，还有一家公司担心与之相关的税收问题。

可以想象一下，如果向菲律宾、俄罗斯和阿根廷的员工以便捷如发短信一般简易的方式发放工资，当天晚些时候，菲律宾员工就能用刚收到的工资，去为他的孩子买一直想要的球衣，这是件多么惬意的事。Bitwage正努力创建一个当前银行系统和支付方式的替代系统，立志于给人们财政上的自由。

Bitwage系统希望能够为全球25亿人提供最无缝且自动的支付方式，将他们带入数字金融系统，而且，Bitwage希望将世界各地的雇

主、雇员和自由职业者从缓慢、昂贵且低效的国际外汇寡头垄断的深渊中解救出来。

2.项目进展

2015年4月，Bitwage与Xapo合作发行了世界上第一张国际比特币工资借记卡，这是将比特币应用于上班人群及日常生活中所迈出的一大步。Bitwage的创始人乔纳森·切斯特（Jonathon Chester）表示，之所以发行比特币借记卡，是因为目前的比特币金融圈中缺少了这一环——工资借记卡。一旦某天比特币被广泛采用，那么借记卡必然要成为比特币金融领域的一部分。

这张比特币借记卡能够提供两方面的服务。第一，它能够帮助使用工资借记卡的企业减少管理费用，并且减少员工发放工资的等待时间。第二，它能够为消费者提供更便利的消费服务，消费者只需要在读卡器上确认一下就能消费，这就省去了在实体店里使用比特币的烦琐程序。虽然此次合作还处于测试阶段，但任何在Bitwage网站上注册的用户都能获得一张免费的比特币借记卡。该卡目前已经在170多个国家推行使用，并且已经应用于以这些国家当地的货币发放工资。虽然该卡目前还不能在美国使用，但是两家公司保证该卡在不久的将来一定会在美国推广。

2015年11月，Bitwage完成了76万美元的种子轮融资。马克思·凯瑟（Max Keiser）的Bitcoin Capital Fund购买了Bitwage在BnkToTheFuture.com上发行的股票。参与投资的公司和个人包括Cloud Money Ventures（比特币公司Uphold旗下的风投公司）、Saeed Amidi（Paypal和Dropbox的早期投资人）、法国电信集团Orange、Draper Associates等。在这段时间，Bitwage还加入了由法国电信巨头Orange在硅谷创办的创业公司加速器项目。

Bitwage的创始人乔纳森·切斯特表示，公司将利用这笔资金来建立

自己的基础设施，尤其是扩大公司在欧洲市场的业务。Bitwage团队计划投入一定的资金来提高用户体验，简化用户整合的过程，让客户更容易整合Bitwage的技术。那些参加Bitwage近期融资的投资者称赞Bitwage具有实际作用，能够推动比特币的使用，这也是他们投资Bitwage的原因。

2016年3月初，Bitwage宣布与一家知名保险公司展开战略合作伙伴关系。不过，Bitwage发言人并未透露是哪家公司，只是表示这是一家规模非常大的企业，并且既不被Coinbase使用，也不被Xapo使用。凭借Sun Microsystems安全部前首席技术官乔尔·魏泽（Joel Weise）的帮助，Bitwage已实施其安全策略。

Bitwage指出，他们的安全标准向ISO（国际标准化组织）与NIST（美国国家标准与技术）的标准以及“业内金融服务机构的最佳做法”看齐，包含用户数据的银行级别加密、严格的密码管理政策、获得所有敏感数据与流程的双重认证以及年度审计（含自身企业总部大楼的实物审计）。Bitwage的安全策略与流程正在接受顶级网络责任保险专家的严格审查。该企业还曾通过保险公司针对网络攻击的检查，并获得A+的AM最佳评级。

Bitwage宣布不存储比特币清单，也没有持有客户资金。这意味着资金只能在很短的时间内被持有。基于此，因恶意行为而产生损失的风险被降到最低。此类支付薪水的方式是个体努力与勤奋工作的绝佳体现。随着不断改进与加强他们的安全计划，Bitwage希望以最大的关怀与最高的安全级别来处理整个流程。

同月，Bitwage表示支持企业借记卡和信用卡发薪系统。用户可以将借记卡或信用卡绑定到Bitwage账户，这样发薪方式就不只局限于比特币和传统电汇，这个新的发薪途径规定每月限额500美元。公司创始人乔纳森·切斯特说，公司对一些收单机构挑选研究，最后确定了一家，但是拒绝透露公司名称。

公司推出这个服务是针对客户反馈做出的决策，继而推动了信用卡和借记卡支付的发展。**Bitwage**关注的是，怎样给公司用户带来最大利益，无论是进行国际薪资支付的企业还是使用个人工资表系统的用户。**Bitwage**认为，现有薪资支付市场给企业提供的卡类支付选择很少，这给创业公司带来了机遇。鉴于企业需求带来的机遇和解决方案的贫乏，**Bitwage**希望开始探索更多可行的办法。

与该项目一起启动的还有**API**项目，并于10月进行了**beta**测试。目前，**Bitwage**已经整合了**API**项目与员工监控服务项目**Hubstaff**。

（三）Colu

以色列初创公司**Colu**旨在通过区块链技术来分配物品的所有权，致力于让那些不懂比特币的开发商和消费者也能够通过该平台建立和交换资产，包括从金融资产（股票、债券）到记录（证书、版权、文件）再到所有权（活动门票、代金券、礼品卡）。随着平台测试版的推出，个人开发者和企业都可以根据自己以及客户的广泛需求，在**Colu.co**上开发相关的数字资产和服务。

Colu成立于2014年秋天，在很短的时间里，**Colu**就已经与超过20家公司建立了合作关系，包括音乐平台**Revelator**、加勒比比特币交易所**Bitt**，以及跨国咨询公司德勤。

简单地说，**Colu**提供给你一种便捷的方式来使用区块链技术。你可以使用代币来交易任何东西，从汽车、艺术品到演唱会的门票。比如你买了一张演唱会的门票，一般而言你拿到的会是一张打印出来的门票，但是现在你收到的将是一串随机数（一张加密令牌）用于验证你购买了门票，而这是通过区块链来实现的。你将得到一组私钥，然后你就可以访问到自己的门票。**Colu**会将这个代币置入到一个二维码内，你可以

通过自己的手机扫描后访问。由于它是数字的形式，你也可以将其传递给别人。

Colu的创始人阿摩司·梅瑞（Amos Meiri）最初从Colored Coins.org入手，这是一个为比特币区块链创建数字资产的开源标准协议。Colu就是基于这种想法的延伸，它既是开发者的API工具，也是一种应用，可以让消费者访问现有比特币框架上的彩色币（Colored Coins）。它允许你在线购物，然后通过区块链进行验证。比如你买了艺术品后，就会明白这件艺术品就是你的了，你将得到一个基于区块链技术的代币证书，而这种数字证书将比纸张证书保存的时间更为持久。Colu是一个应用程序，但不是钱包，你需要将代币存放在其他地方，比如你的计算机或者手机内，又或者U盘之类的地方。除了API以及消费者应用的功能之外，梅瑞还表示他们计划推出一个可以让人们使用区块链技术来买卖货物和服务的市场。

Colu的目标就是继续维护和开发工具以及产品，让开发商和企业体验到比以往更加方便简单地整合区块链技术的方式。由于比特币区块链技术的不可知性，Colu也计划在其他区块链上建立平台。Colu在今后将会发布更多的整合应用，包括金融、记录和所有权。

2015年1月27日，Colu宣布获得250万美元融资，投资方包括Aleph Capital、Spark Capital、BoxGroup以及Bitcoin Opportunity Fund。

Colu还宣布与Revelator进行合作，帮助Revelator建立一个所有权管理API。Revelator是一个基于云技术的信息提供商，为独立音乐公司提供销售和市场情报。在目前音乐的数字化分布中，仍然存在着一个复杂的权利归属和使用权链。这个API将为数字资产的发行和分配提供安全渠道，包括音乐作品的上市和注册，并能够为所有市场参与者收集和提供更高的透明度和效率。

Colu表示在2015年8月将推出区块链公测项目，并且与跨国咨询公

司德勤达成合作协议，这次合作将为区块链技术带来全新的“大市场”。尽管该公司没有公布此次合作的细节，但是该项目将涉及Rubix软件平台，德勤客户可在该平台上建立自己的应用程序，包括在区块链上建立票务系统和登记系统。

第五章 区块链在非金融行业的应用

一、区块链+医疗行业

（一）解决医疗最大的问题

除了金融行业之外，现在看来受益于区块链技术最大的行业应为医疗行业。因为病人的医疗记录和信息在任何时候都是需要予以保密的，而中心化数据库和文件柜都不再是个可行的选择。区块链技术提供了一个可行的替代方案，这是一个能做到完全透明却又能尊重用户隐私的方案。在过去，我们经常会由于一些内部失误，导致患者的信息被泄露。

考虑到所有和健康相关的敏感资料：身份特征、疾病情况、治疗方案以及支付情况，一个人的健康状况可能是其最私密的信息，但是在过去，这些相关信息往往出现过一次又一次的大规模泄露，导致个人健康数据被流传到互联网上。

下面是两个大规模数据泄露的例子：

Anthem：8000万病人和雇员的记录；

UCLA Health：450万病人的记录。

在这些数据泄露的例子中，往往是由于网络操作的问题引起的，使所有的数据暴露在黑客的面前。一个单点故障就能够导致所有人的信息遭到泄露。

而随着个人健康数据越来越多，不同于如身高、体重、血糖、血压之类的传统数据，一些其他重要数据已经到了绝不能泄露的地步。最典型的例子就是指纹数据或者虹膜数据，如果这些资料出现大规模的泄露，会产生非常深远且具有灾难性的影响，考虑到有太多支付方案牵涉指纹支付，也就是说一旦大规模泄露可能会引起金融上的灾难。它不同于密码数据，一旦泄露可以通过大规模修改来避免更大的损失，大多数类似于指纹数据或者虹膜数据是无法随意修改的，这产生的影响将会深远得多。而随着基因数据采集变得越来越容易，我们甚至无法估量基因数据一旦大规模泄露可能带来的灾难性后果。

这种破坏性远比苹果公司的明星私人照片泄露还要大得多，如果连苹果这样闭源的系统数据库都可以泄露，其他中心化的数据库其实同样都存在类似问题。这其中最大的问题就是由于单点故障，或者单把私钥的泄漏导致数据库安全防线的整体性崩溃。因此，很多业内人士认为区块链是人类现在能想到的唯一解决方案。

对医疗行业来说，区块链有三个很重要的优点：首先是高冗余，因为每个节点都有备份，这使单点故障不会损害数据完整性。其次是区块链上的数据无法被篡改，这对于医疗数据非常重要，医疗数据一旦被篡改很可能会导致重大伤害，而且在区块链上的任何篡改都会留下密码学上的证据从而被快速发现。除此之外，区块链最大的优势就是，区块链技术能做到多私钥的复杂权限保管。比如，通过智能合约技术可以设置单个病历分配多把私钥，并且制定一定的规则来对数据进行访问，同时必须获得授权才能够进行，无论是医生、护士或者病人本身都需要获得许可，比如让只有一个或者多个人同时到场才能打开，还可以和GIS（地理信息系统）数据结合在一起，当你在某家医院时，该医院的医生才可以读取病历，也可以和时间信息结合在一起，在某个治疗时间段内相关医生护士才能够读取病历。

区块链的保管方案不同于传统中心化数据库的保管方案，第一次不

需要依靠相信人或者相信制度来确保安全，完全通过算法来确保数据库的安全性。从算法上就杜绝了由于单把私钥的泄露而导致数据库的整体崩溃。

对于区块链和医疗健康领域进行结合，其中最令人感到兴奋的原因是这完全是一个全新的领域。随着企业和医疗机构看到区块链技术对于金融领域的影响，医疗机构将会在医疗健康领域中逐渐开始推广和实施该技术，并且希望获得金融级的安全和效率。目前，全球医疗市场份额有1.057万亿美元，主要的份额占有者包括瑞辉（474亿美元）、强生（163亿美元）、复迈（118.4亿美元）和诺华制药公司（494亿美元）。匿名交叉竞争引用了大量的动态医药数据和历史医疗记录，这种竞争也会给药物发现和个性化医疗开发增加收入源流。

此外，生物识别技术融入量化数据（如运动追踪器的数据），同样能够加入到健康区块链中，区块链技术带来了许多机会来改善现有流程和商业模式，包括现有数据访问、通用电子医疗记录（电子病历）、数字健康资产保护、健康代币甚至是基因钱包等。

（二）未来场景

可以先跟随一名长期患有“苹果综合征”（该病是虚构出来的）的患者开始一段区块链旅程。

首先，我们假设“苹果综合征”是个非常复杂的病症。这种病不会致命，但是它的症状会让人衰弱，可能引起失眠或短暂性失忆。但是它是可以治疗并且能够痊愈的，尽管恢复的过程非常艰辛。

小静是个80后，从事动画师的工作，是个普通的上班族。某个星期四下午，她刚刚完成一个极具挑战的场景后就已经筋疲力尽了，她决定休息一下。外面风景很美，所以她准备出门在河边跑跑步。差不多跑了

两英里后，小静忽然感觉到恶心和头昏眼花。她放慢脚步，但沿路走了100米左右就晕倒了。一个迎面过来的跑步者发现小静昏倒在地上就拨了120急救电话。

当救护车到达时，急救医生扫描了小静手腕上的健身手环来检索她的健康链ID（Health Chain ID），这是一个专门用来记录医疗信息的公共识别符。当小静注册Health Chain时，就创建起了一个规则，这个规则规定了谁能通过验证来访问她的医疗记录，她还给这些人命了名。急救医生结合小静的ID和他们自己的ID，证明他们是受认可（可访问）的急救人员。接着急救人员在Health Chain网络中发布广播，广播会自动向小静的四个紧急联系人发起警告，要求他们确认急救人员可以访问小静的记录。10秒钟后，她的两名紧急联系人确认了急救医生的访问，急救医生便能够访问她的紧急医疗信息了。

几个小时后，小静在医院中醒过来。她很好，但是很惊讶到底发生了什么。候诊医生向她解释说她是患上“苹果综合征”了。检查之后，医生询问她是否愿意在公共研究库中分享她的匿名信息，因为这是标准惯例，她对此没有疑义。她愿意分享她的医疗记录、刚经历事件的相关资料 and 医生正进行测试的结果。

小静想了解和她一样有“苹果综合征”经历的人以及她究竟如何才能痊愈。于是，她和其他人选择加入到一个私人网络中来共享信息。相比于自导式搜索，医生根据她的信息进行了一次标准匹配，选出了一批与小静的重要特征完全相同的人，包括年纪、地理位置和工作类型。

尽管“苹果综合征”频发，治疗该疾病的药物也有所发展，但是康复仍然很难，并且治疗的基础条件不足也没太引起医学界的关注。小静自己对这种情况也做了一些初步的研究，她发现，为发布治疗方案的人提供一些公开的众筹奖金也许能从根本上解决“苹果综合征”的医治问题。小静的捐款由一系列智能合同管理，这些合同在发布时会提供有条件的治疗访问。与传统众筹不同，在她准备使用某个治疗方式之前，她的捐

款由合同保存在第三方那里。

现在小静对自己的情况有了非常透彻的了解。她开始去看专家，专家让她每天进行体育课程，同时还配合服用知名的治疗“苹果综合征”的药物。坚持这两项对于康复很重要，同时小静也获得了保险公司奖励。通过一个可以追踪她位置和活动的手表和可以检测的药物来收集数据，保险公司和医生就能够获得所需要的数据信息了。只要小静坚持双方协定的治疗方案，所有账单都可自动支付，不需要纸质的证明。

由此我们可以发现，医疗和区块链其实是非常匹配的。同时，还能够引导以患者为中心的改革，比如我们应该怎么照顾自己和别人。在我们最脆弱的时刻，我们能够无障碍地与他人共享自己相关的重要信息。我们可以预先承诺给我们想要的治疗方案进行支付回报，而保险款的支付将在我们医疗行为被证实之后触发。其实我们的医疗离现代化还很远，一些高科技还没有被完全运用到医疗的追踪、诊断和治疗上。如果同时利用区块链的话，那么就可以大幅度地改变这一现状。

（三）飞利浦医疗

2015年10月27日，Tierion宣布和飞利浦医疗集团完成首个合作项目，Tierion是一个专门从事数据收集和记录的区块链公司，通过使用区块链记录搭建了一个数据存储和验证平台。

飞利浦医疗保险是一个专注于连接全球数以亿计医疗设备运作的企业。目前非常需要大幅改变病人的医疗状况，但是这一过程需要很长一段时间才能够被实现。而采用区块链技术也许将有助于实现这一目标，比很多人所期待的更早。尽管该项目的细节尚未公开，但飞利浦全球创新IT主管阿伦·莱文（Aron Laeven）告诉记者，“正如我们探索其他的新技术一样，我们正在探索区块链技术在医疗护理领域中的应用”。

在与Tierion合作的6个月时间里，对于飞利浦而言，已经取得了不少进展。于是在2016年3月4日，飞利浦医疗宣布建立区块链实验室来继续推进研究。这样能够联合更多其他公司的IT专家、医疗保健专家和区块链技术开发者推进这方面的研究。该研发中心位于阿姆斯特丹，专门用于研究新兴科技。飞利浦指出，他在寻找合作伙伴和开发者来合作这个项目。公司还特别暗示，飞利浦相信区块链技术适用于医疗保健行业。

很多年来，飞利浦医疗已经在该领域上有了一些有趣的突破，使医疗服务变得更加方便——并且能够让人更负担得起——为发展中国家弥补了这个缺口。但是，这还不是全部，病人健康信息的实时监测也许才是其中的首要任务。和大多数医疗护理企业和机构相比，飞利浦医疗更重视以人为本，非常重视病人的反馈。通过引领该领域取得更多的创新，让医疗保健的患者们每天的生活变得更有意义。

所有由飞利浦健康所提供的产品和服务都有可能通过整合区块链技术来获益。也许这就是Tierion所带来的创新方案，即能够提供一个去中心化的实时信息监测方案，它能够解决以前中心化存储数据方案中所不能解决的（信息安全）问题。Tierion提供的以区块链为基础的数据方案，同时也能够给其他行业的企业带来好处。

（四）Gem

2016年1月，区块链企业Gem宣布获得了700万美元的投资来扩展它的企业平台，并已经和健康行业内多个不同利益相关方进行合作，来评估是否需要区块链技术。Gem首席执行官麦克·温克尔施佩希特表示，类似于金融行业，设计一个区块链应用，需要考虑医疗健康行业内多个相关利益者。如果能够将每个独立相关方都链接到一个有凝聚力的、可以共享读写的数据库的话，那么真正的区块链创新将会产生。如果能够

让保险公司、医院结算部门、贷款人和病人共同使用一个区块链来管理支付，那么在整个行业中就会大规模地减少冗余。

另外，区块链网络绝不仅仅用于解决医疗健康数据保存问题，收付款将会是另外一个发展方向。如果区块链能够在管理医疗付费的整个过程中被使用，那么也将能够管理病人医疗记录的整个过程。区块链能够让其他多个组织来访问网络，而不需要担心数据的安全和完整性。病历可以被多方进行创建、共享，并且能够让多方进行追加更新，这将会重塑整个行业的效率和透明度。

2016年4月27日，区块链技术服务提供公司Gem发布了Gem Health项目，该项目目的是通过新兴科技促进医疗领域间的合作。其首个合作伙伴就是飞利浦医疗，飞利浦医疗会帮助其搭建一个私人以太坊区块链，来开发企业医疗的应用程序。Gem希望通过此项目可以鼓励医疗行业通过区块链技术开发出更多健康应用程序、全球病人身份识别软件及安全电子医疗记录。

Gem正在发布一个可以让医疗公司参与实验及构建跨行业应用程序的网络，来解决不同问题的应用案例。Gem正在帮助大量孤立运作的公司创建一个良好的合作环境，且正在投资该行业的通信渠道和与身体健康有关的项目。

Gem最初的定位是比特币初创公司的API供应商，而通过此次项目又开发了为企业提供服务的业务。Gem现在把自己定位于为从事区块链领域公司提供咨询及匹配服务的公司。Gem表示，这是一个非常大且非常重要的机遇，医疗健康影响着我们每个人，通过这次机会有可能改变整个行业。

（五）Factom

Factom和HealthNautica正在寻求安全的医疗记录和审计跟踪解决方案。他们通过数据加密写入比特币区块链，并且通过时间戳来确保数据的精确度。这些记录完全无法被篡改，因为它是写入到区块链中的，并且在没有权限的情况下是无法进行阅读的。HealthNautica希望能够提升赔偿流程的处理效率和记录无法改变的确定性。

（六）爱沙尼亚

2016年3月，爱沙尼亚宣布启动基于区块链的医疗健康档案安全项目。爱沙尼亚在区块链投入和应用方面一直要远远领先于其他国家，尽管它只是波罗的海的一个小国，但很早就开始与BitNation进行合作，将区块链技术应用于居民的身份验证。并且在2016年初，纳斯达克在爱沙尼亚的交易所，已经开始使用区块链进行股东的投票。而这次，则是把区块链应用扩展到电子健康档案的保管。

数据安全初创企业Guardtime宣布与爱沙尼亚电子卫生基金会合作（Estonia eHealth Foundation），利用区块链技术保证100万份病人医疗记录安全。该基金从此整合了Guardtime的无钥签名基础设施区块链技术（Keyless Signature Infrastructure, KSI）和基金会Oracle数据引擎，以实现实时查看病人病例。

爱沙尼亚早在1997年建立这个电子政务系统就引起了人们的关注。其实现方式是在身份证内嵌入芯片，然后国家公民就可以使用100多项电子政府服务，例如纳税申报、投票。整个服务过程是即时的，仅仅需要登录一个网站。爱沙尼亚的电子政务系统内包含了电子病人记录。而整合Guardtime技术的目的就是用“独立的法医品质的审计线索”保护这些数据安全。由于黑客、恶意软件、系统问题等的存在，敏感数据保护中存在的安全隐患包括信息篡改、删除、错误升级等。而区块链技术可以保证数据的真实完整，并能完全记录数据变更过程。

（七）IBM

2016年5月，IBM的区块链云服务升级，其目标锁定政府和医疗保健行业。IBM研发出一个新的框架，用于保护其云服务平台上的区块链系统，并认为它可以帮助金融企业满足监管和安全要求等限制区块链技术发展的因素。IBM区块链部门副主席杰里·柯摩（Jerry Cuomo）说，新的框架是为了“加快”区块链应用步伐，消除这些缺陷和提高开发者的应用体验。

IBM认为现有公共区块链很安全，只是受限于严格的数据保护要求而无法适用于商业领域。商业要求数据一致性，公共区块链有精密的算法；但是这些架构中的区块链存在变化，也就是说存在两个版本。而在商业中，这种不一致是不能容忍的。

IBM相信该框架可以帮助机构创建用于许可型区块链的“安全云环境”，突破行业的安全和合法性要求，对行业发展极其有利。该框架受益人包括政府或医疗保健服务供应商；因为他们希望利用基于区块链的系统来满足联邦信息处理标准和健康保险流通与责任法案的要求。

（八）美国国会

2016年5月中旬举行的美国国会会议中，经济智囊团代表提出区块链技术可以完善新一代的医疗卫生数据体系。美国企业研究院（AEI）的斯科特·戈特利布（Scott Gottlieb）提出，从某种程度上说，要想使美国保险市场有创新和竞争，科技的力量不容小觑。戈特利布建议建立一个在技术上更先进的风险池，能够实现保险津贴的自动化管理，而AEI认为，这项技术就是区块链。

一份完整的保险统筹方案，通常包含了民众的津贴调整和个人医疗

状况等信息，而这些信息通常都属于个人隐私，这就需要完善的信息登记系统来保障信息的严密性，但同时还要授权其他机构（例如医院）调取这些信息。区块链正好符合以上所有要求。

近年来，美国大力实施《平价医疗法案》，也就是“奥巴马医改”。目的是为没有医疗保险的美国公民提供医疗保障，建立全民医疗保障体系。这个建议提出后，美国政府目前正在联合飞利浦和区块链创业公司Gem和Tierion，计划建立一个区块链研究实验室，积极研究区块链技术的可行性。

二、区块链+保险行业

（一）如何与传统保险连接

人们对于风险的观念很可能受到技术变革和应用的影响，比如区块链。现有保险行业的主要业务模式就是一个有足够资金支持的中心组织，并与个人订立合同关系。而区块链应用很可能会改变保险公司这种提供互惠关系的方法。通过基于区块链的点对点互助保险平台，区块链技术可以让人们更加直接地管理他们的风险，而且只需要部分资金支持。回顾一下其他行业的共享协作案例（比如Uber、Airbnb），如果应用于保险行业，这种情况下，保险公司的角色就逐渐转变为专业咨询和互惠池机制管理，而不是直接吸收风险。这种技术也可以支持普惠金融，以及个人与保险提供商之间互动的新模式，最终有利于提高客户满意度、忠诚度、信任度、透明度和可靠性。

区块链技术的出现可以促进合约自动化的进程，通过使用智能合约来实现效率的提升，并使某些保险产品随着时间的推移实现自我管理。另外区块链也可以做到高效地解决索赔和减少保险欺诈——各方都可以使用区块链验证各方信息（当事人核实保险的真实性，保险公司审核当事人和事件，如车祸、期债行为等）。这将极大地提高彼此的交互信任。此外，这种交互式的保险也会增加对保险的需求和传播，减小保险行业中再保险的概率。

区块链技术可以提高保险产业的安全性，并且将极大地降低保险公司的经营成本。根据美国财务部的统计，至2012年底美国保险公司持有7.3万亿美元的总资产。由于保险公司持有极大的资产，而要管理这些资产所付出的成本恐怕也不容小觑。因此，区块链对保险行业的应用，

将有着重要的经济意义。

现阶段，有三个领域值得主流保险公司关注。

第一，他们可以试着建立私有区块链，不与比特币或者其他区块链连接，作为抓手与客户和监管机构讨论未来将如何发展。

第二，他们需要探索私有区块链如何运营和收费，可以在不同协议和经济机构上做实验。

第三，他们不但应该严格审视现存信息技术架构，而且应该审视他们现有的和未来的产品，看看产品和风险管理方面，哪些地方可以使用区块链技术或者相关应用进行改进。每一家人寿保险公司的核心系统都是一个居于核心地位的，庞大的中心交易账户。最起码作为今天集中式数据库模型的可能替代方案，区块链值得保险公司在技术上进行评估。

大多数保险公司并没有准备好在区块链技术上进行实验。他们发现比特币或者数字货币理解起来很困难。而非保险机构更可能首先创建保险或者与保险相关的应用。保险方面的区块链应用很可能从数字身份识别系统和个人数据管理开始。

区块链与个人保险相关的有四个不同业务领域：身份认证、空间、时间，以及互动。其中每一个领域，都将给保险行业提供一个新机会。

1. 身份认证

区块链技术和相关应用能够改变我们管理数字身份标识、个人信息和历史的方式。通过基于去中心化区块链，结合保存记录的公开账本，以去中心化和密码学的方式，保护隐私的力度足够和政府所使用的身份管理方案相媲美，第三方机构比如保险公司甚至是分布式声誉评级机构都需要获得使用数据的许可。政府身份管理方案通常是比对多个数据库，或者使用指纹等生物数据。

这个身份解决方案能够填补数字身份验证和认证方案之间的空白。目前已经有很多团队在努力研究类似的可识别验证的身份系统。社交媒体网络也正在寻求数字身份的方式，但是通常不能满足大多数无须验证的基本信任需求。目前出现了不少数字身份的方案，包括OpenID链接，这是一个将身份协议层和认证服务器结合的方式，在不需要持有和管理密码的情况下，能够让各类客户（包括开发者）跨网站和应用来请求和发出认证信息。政府部门也在建立自己的数字身份系统和验证流程。以英国政府为例，在2014年9月其推出Gov.UK验证，这是一个公共身份验证服务，使用收信人的网络和第三方服务提供来替代目前的中心化数据库，该系统目前还在测试中。爱沙尼亚运营一个数字身份的方案已有十多年，目前计划将该方案扩大到非本国居民，如果其他国家也能够通过它进行识别，那将使该方案不再局限在单一国家。

使用数字身份系统的主要问题是，是否可以被信任，并且能够被广泛使用。在实践中，以区块链为基础的身份方案可以建立一个去中心化协议上的分布式应用，使用仲裁员方式（如预先设定专家认证文件或信息资料）或者使用不同信息源（包括政府数据库）来交叉确认信息安全。这个应用还能提供更多额外的功能，包括个人数据存储、为外部提供认证框架，甚至是信誉评级。

这些功能可以扩展到已经被开发的私人数据（例如Meeco，这是一个免费广告平台的私人数据管理解决方案）。集合验证和个人数据管理功能，通过去中心化管理和安全的区块链技术可以建立身份管理的全新框架。如果成功的话，这种身份识别方案可以消除政府在身份认证、存储和管理方面的垄断。此外，将可以让个人能够存储和管理他们自己的数据，还可以访问个人历史记录。

个人不再需要可信的第三方存储或者管理他们的信息。这些应用可以减少识别和声明欺诈，增进对产品的信任，降低费用，从而提高市场占有率。区块链技术扩展了可被去中心化存储和记录的事物范围，有意

思的应用可能出现在这些相关领域，如事故、健康数据记录、日常数据和相关的认证功能等。绝不丢失数据的理念将改变社会对身份识别、隐私和安全的看法。

首先，个人身份识别和验证，以及数据管理对于许多行业都有莫大的好处。在保险领域也是如此，数字认证可以让保险公司和个人之间更好地管理大数据和历史记录，让这个过程变得更加直接和有效率。随着时间的推移，因为身份问题导致的欺诈风险将会降低。区块链技术可以促进个人医疗健康的记录存储和管理并且帮助个人来管理类似于医生访问这样的第三方访问权限。其次，区块链可以支持医疗共享数据的研究，通过汇总区块链上个人自愿提供的健康档案数据来为研究提供庞大的样本，这样区块链匿名的优势就能够体现出来。最后，区块链可以为保险、测试结果、处方、转诊证明等各类健康相关的数据证明。这种数据驱动的分布式方案对保险公司、产品和流程是非常有利的。

就目前而言，访问和控制自己的数据变成越来越敏感的问题，增强个人存储、更新和管理访问他们的数据的功能变得越来越有吸引力，尤其是涉及医疗保健方面。假设你有一个便携的、安全的、全球可用的个人数据存储区块链里，任何时候都可与可信的第三方分享健康记录或者驾驶记录。你可以将健康记录提交给一位新医生或者得到一个人寿保险报价，或者可以将驾驶记录提交到机场柜台，从而获得汽车租赁安全折扣。你的个人数据存储记录也许包含你的生物特征数据，这样你就可以在任何时候证明自己的身份。

2.空间

在空间方面，区块链是在计算机网络上以分布式形式存在的，它们可以分布在全球数字空间的每个角落。区块链技术能够重塑个人和空间之间的不同作用，也许将会进一步模糊本地和全球之间的差异。区块链技术和相关应用，本身规模和影响范围就是全球的。从用户的角度来

看，唯一的要求就是拥有一台可以接入互联网的计算机或者移动设备即可。与此同时，区块链应用程序能够满足全球各地任何人的特殊需求。

这个空间领域的双重关系可以让保险产品以两种方式存在：一是通过扩大保险产品的空间范围；二是通过调整保险覆盖范围和具体地点时间来调整价格。前者可以让保险产品之前不具备的金融包容性成为可能，例如在某些地方没有足够强劲的市场需求，或者没有足够的质量数据支持（如信用数据）。后者表明区块链技术能够作为“大数据”解决方案的一部分，包括能够远程连接设备（物联网），通过更加全面的数据，以及横跨空间和时间来进行深入分析，实现实时地调整保险范围和价格，这样可以极大地提高效率。

传统的保险模式是非常中心化的，有固定的范围（如一个保险企业总是有固定的国家、市场、地区）。区块链技术可以实现“去本地化”，点对点的商业模式和互助保险，都让位置这个因素或多或少变得不再这么重要。好处是，人们彼此能够使用强大的技术来建立合约，也可以更容易地建立本地企业保险。同时许多地区的车辆可以共享来自全球的准备金或者再保险服务。

3.时间

区块链技术的“时间戳”能够记录区块链整个时间周期内的交易记录和“交易值”。区块链和时间之间有两种相互作用需要区分。第一，区块链技术能够增大时间的范围并增加各种可能性，如能够将过去保险合同的时间分成多个部分，并且让多种产品进行组合。例如，就像前面所指出的，分布式应用能够根据情况，进行自我管理，实时调整保险覆盖范围和策略。此外，区块链技术能够让多种保险产品具有不同的时间跨度，例如建立超短期保险合同或特定时间范围的保险合同。因此，区块链技术能够缩短时间周期，通过裁减不同保险产品的时间来施加影响。

第二，有一个看起来和第一个特点相反的优势，区块链技术由于能

够让记录在区块链整个存续时间内进行保存，所以让人感觉似乎会是永久不变的，时间像是被延长了。这些记录是不会随着时间而更改的，但是其内容（所记录的交易）可以进行转移。例如，记录在区块链上的资产信息是无法篡改的，而且是永久地保留，但是这个资产是可以转移到其他用户那里的，这些记录的长久存在和精确度，可能会让人改变对于长期合约的看法，会极大地增强对于长期保险合约的信心。

通过分布式应用，自我管理的风险协议能够跨越时间和空间，调整保险覆盖范围来施加影响。最大的挑战是如何能够创建正确的区块链保险模式，一开始我们可能会从最熟悉的风险（如车祸）和相关的保险产品（汽车保险）开始入手，或者有机会扩展这些风险，例如共享经济带来的Uber和Airbnb这些全新的商业领域。

4.互动

建立于区块链之上的智能合约，使投保人能够自行管理自己的保险产品。智能合约能够自动有效地处理保险过程，改变相关公司的业务方式。区块链技术可能有助于保险业中的主要模型由风险共担向替代型风险管理模型的转移。基于区块链的风险管理模型，可能包括自我管理、风险管理协议，点对点保险平台，甚至是充分的资金解决方案。

假设有些人现在可以创建他们自己的风险池系统。这些可能是即时的微保险或者微互助，是一种对于保险的互助经济尝试。广大家庭可以互相提供互助健康保险，这种保险包含联合互惠安排，可能是不相关的中国乡村健康计划或是一个标准的国际再保险产品。这个再保险产品是由一个全球再保险公司专门为这些家庭计划而开发的。如果保险公司不再需要为风险设立基金呢？比如，人们可以更容易得到可调整的赔付资金池，以反映风险水平的变化。失业保险可以融合教育贷款和终身协议，这样年轻人就可以得到教育方面的资金支持和失业方面的保险支持，与此同时，他们上班时工资薪金的一部分就被用于覆盖其他人的风

险了。

（二）保险DAO

更彻底的是，基于智能合约的“炫酷产品”最可能应用于保险新领域（比如互助保险产品），或者应对由区块链技术应用而兴起的新风险（比如数字资产保护），而不是替代已有的产品。

基于区块链的保险业解决方案，也可写成一组规则，并转变成一个DAO，使消费者能够不再依赖中间人。区块链技术将最终促使保险公司社会角色和功能的变化。例如，通过分布式微型保险解决方案，人们可以获得价格合理质量相当的保险产品；或者通过扩展保险产品，为之前被排除在外的人群提供足够的身份管理和信息管理功能。随着时间的推移，区块链技术也将进一步扩大保险市场规模。传统保险行业也能通过区块链智能合约使某些产品达到自动化。

在这个新的商业模式中，保险公司关注的焦点会由资产管理（而不是供需匹配）转变到风险计算研究。保险公司会提供一个类似于市场的平台，在这个平台上消费者可以说出他们的保险需求，可以是标准化的产品或是某一特殊需求。保险公司会根据历史数据，使用其“风险智能”或风险模式，在减去保证金之后，根据保费计算方式计算出预期回报。在公布保费计算方式之后，感兴趣的投资者可以竞标或订购想要的保险服务，也可以通过集体众筹或个人P2P的方式。这都取决于保险需求的种类、投资者可用资源和他们的风险喜好。

除了去中心化账本中的管理，若客户提出保险索赔要求，通过使用智能合约，可以确保投资者能够偿付给客户。智能合约被设定为传统的保证书，但是不需要经过银行。通过区块链技术，管理和执行过程也会变得更简单，传统公司的业务更加透明，成本更低。保险公司同时可以

验证保险索赔的有效性，可以通过连接区块链到其他账本，以及外包给第三方，这样就可以自动验证了。

在这个模式下，在保险市场下智能合同的使用范围就不会局限在P2P的保险形式下了，而是几乎可以应用在所有保险形式中。如果一个人联合所有愿意通过众筹模式投资的投资者，就可以减少紧急事件对每个投资者的影响。

这个新的商业模式对所有人来说都是有利的，包括保险公司、投资者和消费者。资金可以留住投资者的客户，反过来说，保险公司可以通过少量的资本甚至不需要资本进行操控。保险公司作为市场和风险智能的供应商，可以获得许多好处。与P2P借贷公司有相似模式的公司不需要监管许可证，甚至都不需要任何证书，只需要得到监管者的许可即可。平台开发可以按次计费外包给第三方，让公司更加智能，最终成为一个精简有效率的组织。从投资者的角度来看，这给精简组织带来了新投资，同时也有更高的回报。私人投资者也可以加入市场，投资者会对金融风险有更清晰的认识。最后，对消费者来说，由于有大量投资者竞标、订购，以及较少的操作成本，保险费用也会更低。这个模式可以让消费者更容易选择适合的保险，同时智能合同可以使支付更安全。

当然，这个模式要面对许多挑战，最大的挑战之一就是监管者是否允许这些新的有效率的方法在市场中存在。从投资者的角度来看，在偿付高额费用时，为了分散风险，保险公司需要让大量的人参与进来，同时在面对特定保险时，还需要有一定的灵活性。至于风险计算，由于保险的特殊性，保险公司需要正确计算风险回报率，这对消费者和投资者来说都是非常具有吸引力的。消费者的角色也很重要，因为他们需要在没有第三方的情况下信任这个有区块链的系统。

但是，总的来说，这种商业模式是非常有趣的，同时可以带来许多好处，可以创造一个真正的P2P众筹保险公司。有人认为，如果这种商业模式一旦被充分开发，也许就不再有传统的保险公司了，全新的区块

链保险DAO会成为这个行业至关重要的商业角色。

（三）USAA

美国保险巨头USAA开始投入资源来探索如何将区块链技术融入其基础设施。目前，USAA处于早期阶段，正在了解分布式的开放总账如何能够应用于其业务中。

公司虽然尚未确定要如何实现该技术，可能会研究区块链如何才能分散公司的后台运营，但却表示出该公司对区块链技术有着“浓厚的兴趣”。

USAA进军数字货币行业开始于2015年，当时USAA参加了Coinbase的7500万美元的C轮融资。USAA表示没有任何计划接受比特币作为货币，但是看到了区块链可以以某种形式应用于USAA的潜在途径。2015年11月试点方案出台之后，为了扩大比特币技术融合，2016年3月，USAA宣布所有账户持有人都可以从USAA.com界面进入Coinbase平台查看账户余额。据USAA报道，这次试运行很成功，手机端应用可能很快发布。USAA.com和USAA手机应用都是首次实验的一部分。

USAA投资合伙人乔恩·乔拉克（Jon Cholak）说，自己很早就已经支持这个项目了。他表示，“USAA的传统就是善于走在新技术潮流的前沿，我们要开发的项目是金融服务业最先进的”。

（四）SafeShare保险公司

2016年3月下旬，SafeShare保险公司宣布推出基于区块链的保险服务。SafeShare是一家保险服务公司，针对共享经济商业模式，推出了一

个新的以区块链为基础的保险产品。

区块链技术存储了重要的加密交易数据，并且是安全的。存储在区块链里的信息主要用于负责执行交易和防止重复支付。比特币区块链使用SHA-256加密技术保证信息安全。

SafeShare是新时代的保险解决方案供应商，位于英国伦敦，属于Cornerstone Insurance Brokers Limited（基石保险经济有限公司）。SafeShare专门为新成立的共享经济商业模式提供保险解决方案。像Airbnb和Uber这样的应用程序现在很流行。它们都是以共享经济商业模式为基础，以个人名义提供服务，通过应用程序或平台来运行。

这些商业模式（如果可以这样称呼）需要及时划分保险责任范围，当新客户出现时，以提供保险解决方案为基础的SafeShare就是这样做的。根据亚历克斯·斯坦因阿尔特（Alex Steinart）表示，SafeShare使用的区块链技术是由Z/Yen集团创建，使用MetroGnomo开通“时间戳”服务。当维护投保交易时，可以及时帮助公司提供保险产品给客户。

SafeShare通过区块链提供的保险解决方案是由劳合社（Lloyd's）通过24小时理赔热线签署的。除了提供及时便捷的保险方案外，比特币技术同样能帮助保险公司降低成本。

（五）安永会计师事务所

2016年4月15日，安永会计师事务所发布了名为《区块链技术作为数字化平台在保险业的应用》的报告。

保险公司一直以来都对采用颠覆性创新技术不甚积极，其创新战略唯一的目的是维护客户和企业的最大化利益。目前这些企业纷纷开始探索区块链技术，认为该技术的去信任系统可以真正带来长期的战略性

利益。因为它能提供安全的去中心化的交易；精准及时的变动通知可以降低风险，增加资本机遇；降低运营成本；提高企业管理水平。随着技术进步，保险公司控制的活动应该慢慢转变为全新的数字化模型，其技术基础设施也就要相对升级以适应新的生态环境。

新的分布式技术降低了保险公司的技术应用障碍，对现有金融模型构成了一些威胁。区块链技术的潜能可以带来前所未有的行业透明度和可靠性。

安永认为，对保险业而言，区块链主要提供了四大机遇：诈骗探测和风险防范、数字化的投诉管理、新的行业颠覆和资源分配、网络安全责任。尽管区块链技术在保险业的应用前景很好，可是像所有新技术出现的初期阶段一样，该技术的可扩展性、实施技术、与企业 and 政府机构的实际融合都引起了行业的担忧。

监管者担心的是：基础设施还不完善，会给现实技术融合带来隐患；区块链技术人员专业性不够，难以保障各方利益；损失控制机制标准化也还在完善中。

保险公司主要的担忧是：该技术的扩展性以及和现有系统的兼容性、风险管理、计划制定和时机把握。

市场的主要担忧是：中心化基础设施的减少带来高额的监管成本和复杂性；技术发展可能使强制性、规范性监管变得低效；市场需要弹性的审慎监管；欧盟委员会计划提高数据和隐私保护标准；消费者数据控制方式会改变。

总体来说，金融服务机构应该继续加大对该技术的探索 and 开发，创造出适合行业发展的应用。安永也专门成立了核心团队，为企业家和保险公司的发展提供机遇。

（六）John Hancock

2016年4月下旬，保险业巨头恒康金融集团（John Hancock）开启了区块链技术测试。人寿保险和金融服务业巨头John Hancock开始研究多个区块链概念证明机制，探索分布式账本技术重塑现有保险业流程的方式。虽然目前概念证明机制与保险业之间没有密切关联，可是这个于2015年因客户索赔损失246亿美元的公司却在行业内进行了广泛的区块链技术探索，相信将来就会出现实质性的保险业应用。

John Hancock发布和管理着很多金融产品，包括人寿保险、年金、投资品、401k计划、长期护理保险、教育储蓄以及其他多种商业保险。他们的团队正在进行区块链应用探索，致力于提高公司的透明度和效率，而且更加关注该技术对运行效率和效益的影响。目前正进行“了解客户需求”原则的测试，公司法律部希望通过这个项目简化企业后台运营。

该公司在波士顿和麻省的LOFT实验室（Lab of Forward Thinking）负责开发这些概念证明机制。LOFT成立于2015年5月，7月正式发布，其成立的宗旨是帮助员工开发保险、财富和资产管理技术。LOFT内部头脑风暴会议研究出了几个可行的用例，并且决定联系两家基于以太坊区块链的初创企业，促成了公司与ConsenSys和BlockApps公司代表的交流。目前John Hancock公司的LOFT区块链专题小组有四个成员，探索用区块链技术开发与员工激励应用相关的最低可行性产品，并在2016年6月后发布最低可行性产品，它将包含工作组与ConsenSys和BlockApps合作的教育和平台搭建阶段。下个阶段的工作焦点是研究ConsenSys的咨询服务以及探索更广泛的应用领域。然而这只是John Hancock搭建区块链保险服务庞大项目中的一小步，也是整个行业在该领域的第一步。

（七）IBM

2016年4月下旬，IBM金融论坛在杭州召开。其间，IBM发布了针对包括银行和保险在内的金融业发展的最新洞察，并分享了IBM助力全球及中国金融行业构建认知未来、制胜变革的战略与实践。此外，IBM还对目前大热的区块链技术进行了解读，并展望了融合区块链技术的IBM认知解决方案。

会议提到要拥抱数字化保险。面对数字化时代，保险行业需要从提升客户价值、业务人员效率以及内部运营效率和透明度这三个核心价值入手，着力打造三种关键能力：提供全渠道统一体验，建立认知计算能力，以及打造物联保险生态系统。

IBM拥有包括360度客户统一视图——社交营销以及风险识别iOS APP（苹果系统的应用程序）在内的成熟可落地的全渠道统一体验解决方案。在数字保险时代，认知计算将有两种落地应用模式。第一种是重塑传统业务运营环节；第二种是通过数据洞察和对未知探索的深入，创造更新的商业模式。

IBM大中华区全球企业咨询服务部保险业总经理张育成表示：“所谓重塑运营环节，主要是指对传统业务运营各个环节的智能化改造，包括重塑客户交互旅程体验以及帮助保险公司转变业务运营等，以提高运营效率和客户感知，并最终提升客户价值。而新的商业模式，比如IBM‘Watson’与物联网以及保险的结合，可以产生互联设备大数据的保险和相关生态，从事后赔偿到事前保护，更多地去关注出行、健康、居住以及生产等保障性的需求。”

三、区块链+能源行业

能源领域也是区块链能够改变的产业之一。能源革命正在发生，未来是万物互联的趋势，交易的主体是机器和机器，交易的属性更加高频和低密度。区块链具有分布式账本和智能化的合约体系功能，能够将能源流、资金流和信息流有效地衔接，区块链将成为能源互联网真正落地的技术保障。

（一）未来设想

晚上8点仍然炎热的澳大利亚偏远内陆，一根电线杆突然倒塌，这可急坏了威廉和奥利维·门罗（William and Olivia Munroe）。他们在维多利亚大沙漠边缘旧金矿镇外围100英里的地方圈养了100头牛羊。夏天这里的温度时常飙升到华氏120度，孩子们要参加网上课程，这个家庭获取医疗急救服务的唯一途径也是互联网。面对各种空调、通信和水源需求，家里的备用发电机显然撑不了多久。总之他们一家的生活完全依赖可靠的能源。

9小时后，电力公司派了维修队查找倒了的电线杆。客户投诉时告知了事故位置，但是维修队还是花了一天多时间才检修好。同时，门罗一家和附近邻居、企业、机构一直处于没电、没通信状态，给生活带来诸多不便，增加了经济损失和人身风险。对偏远地区的居民来说，停电可不只是影响正常生活，对其人身也有风险性。因此为了把危险最小化，电力公司需要定期派工程队来检修电网。

想象一下，智能的电线杆该有多安全、方便和实惠。可以报告运行状况，对故障采取相应措施。如果电线杆着火，将很快生成事故报告，

并通知维修队带着适合的工具到确定地点。同时电线杆还可以将电力传输任务暂时分配给附近的电线杆，毕竟它们都属于同一个电网。这样电力公司也就不需要花费相当高的现场检修成本，还可以尽快地恢复用电。

物联网的新软件和技术可以为现有的基础设施提供智能系统，例如可以为电网添加可以互相通信的智能设备。想象一下搭建新的安全、有弹性的网络，可以快速和相对低成本地提供更多服务。

这个结构被称为网状网络——计算机和其他设备之间直接互联的网络。它们可以按照带宽、存储等网络特性来自动重新配置，因此不会损坏或中断。缺少廉价服务或渠道的社区可以用网状网络实现基本的联通。网状网络代替了传统的自上而下的组织、监管和控制模型，而由于整个环节不需要中央组织的参与，其安全性和私密性也更高。

（二）Filament

很多组织已经结合网状网络和区块链技术来解决复杂的基础设施问题。美国区块链创业公司Filament在澳大利亚偏远地区的电线杆上进行了所谓的“龙头”（taps）试验，这些“龙头”可以在10英里之内直接通信；因为电线杆的间距一般是200英尺，故障电线杆上的动作探测器会通知200英尺外的电线杆；假设这个探测器故障，它会按顺序通知10英里内的其他电线杆，然后通过120英里内最近的回程网络与公司通信。

客户可以用手机、平板或计算机直接连接到设备，这个“龙头”包含了很多传感器——温度、湿度、光和声音等，客户可以用这些传感器长期监测和分析电网状况。他们可以获取相关数据信息，并通过授权将数据通过区块链传输给其他用户——政府、广播员、电线杆制造商、环保部门。

Filament的商业模式包括三个参与方——Filament、客户和电力公司。Filament拥有硬件，它的设备一直监控电线杆状况和信息交换，把传感器数据卖给数据集成商，然后再卖给电力公司。电力公司按月支付监控设备费用，减少了现场检查的高昂成本。因为电线杆很少会倒塌，所以网状网络的通信功能基本是闲置的。

因为Filament拥有设备，可以出售跨越整个澳大利亚网络多余的容量，甚至可以与联邦快递合作，联邦快递网点可以用网状网络进行通信和追踪车辆来预计到达时间和故障情况。

未来物联网应用依赖于一个账本——物联账本（the Ledger of Things）。上万个智能电线杆通过传感器收集数据，并在其他设备、计算机和人之间传输数据，因此系统需要持续追踪所有信息以保障其可靠性，包括区分每个电线杆。

没有身份是不可能运行的，用于身份认证的区块链是物联网的核心，Filament为每个设备设定独特的路线，然后把这个路线——身份存储在属于Filament的比特币区块链中；而且这个身份信息可以像比特币一样传输。区块链还可以保证这些设备收到费用才会继续运行，没有区块链的支付网络，物联网不可能运行，而其中比特币是通用的交易语言。

（三）LO3

2016年3月3日，在纽约布鲁克林，一家名为LO3的小公司和区块链技术开发商ConsenSys合资成立了一家新公司，名字是TransActive Grid，新公司在布鲁克林地区运行着一个微网项目，在他们看来，这个小项目很有可能改写能源的交易方式，“在总统大道的一边，五户家庭通过太阳能光伏板发电；在街道另一边的五户家庭可以购买对面家庭不

需要的电力。而连接这项交易的就是区块链网络，几乎不需要人员参与就可以管理记录交易”。

未来的双向电力系统由亿万交互的终端组成，包括微电网、光伏系统、智能设备、分布式计算以及能源管理软件等。面对电网运行环境的不断变化，如何能够实时、自动地验证和确保不同节点之间的海量交易？许多人相信区块链技术可以成为这一系统的技术基础。

LO3能源公司致力于打造“开源且加密安全的”区块链来管理微网上的电力交易。除了一些早期的呈现，区块链在电网的应用很大程度上还处于理论层面。在现阶段，一些先期参与者正在为能源和用电设备设计验证系统。但更多的人埋头于寻找区块链的用武之地以及实现方式。越来越多的人相信，能源领域也是区块链能够改变的行业之一。

布鲁克林的ConsenSys用公开的以太坊区块链搭建可审计、透明的点对点能源交易方式。LO3的另一个相关项目布鲁克林微电网（Brooklyn Microgrid）的目的是将当地社区加入可以独立于大型电网的区域。该电网设备可以记录家庭消费以及由太阳能光伏板产生的能量。其创意是，通过融合微电网概念和TransActive Grid支付基础设施，社区居民可以在区块链上撰写智能合约，并选择自己使用的电能来源、类型，甚至决定将电源信卖或赠送给谁。

TransActive Grid包括了智能仪表硬件层以及使用区块链智能合约的软件层——在以太坊区块链自动执行的合约，以太坊平台提供一个可审计的、无法篡改的、加密的自动交易历史。参与的家庭都有连接到区块链的智能仪表，追踪记录家庭使用的电量以及管理邻居之间的电力交易。微电网中参与者的能源智能仪表数据，可以为ConsenSys代币发行及管理系统创建代币，代表生产消费者太阳能光伏板的剩余电量。这些代币就代表着可再生能源生产的一定数量的能源，可以通过区块链智能仪表钱包进行交易。如果成功了，就可以运用到整个布鲁克林微电网中。目前有130户家庭对此项目感兴趣。Orsini的重点是当地智能能源电

网交易比传统自上而下的能源配电系统更有效率——可以节省整体开支，给全社会带来好处同时展示分布式账本的力量。

“产消者”——既是生产者又是消费者——是新兴股份制经济的流行词。在TransActive Grid概念中，生产消费者可以控制自己的能源：消费者可以选择从邻居或其他可再生能源来源处购买。家庭能源生产者可以把多余的电力卖给邻居，社区可以保存当地的能源资源，减少能源浪费，提高微观电力和宏观电力的利用率。

LO3能源已建立了双节点的模型，在微电网中收集消纳和发电数据，并将其应用到区块链中。由于计划刚刚开始，试验节点仍在正常运行中。

2016年4月11日，区块链迎来了世界首个点对点能源交易。两名布鲁克林居民通过使用以太坊区块链直接完成了一笔能源买卖交易。这是世界上首个使用消费者区块链交易的小型电力网，也就是微电网，这意味着微电网已经开始在纽约使用了。这样的微电网是和国家电网分离的，如果遇到飓风还可以选择其他电网而不至于断电。通过微电网、屋顶太阳能设备安装等方式充分利用能源效率，在给客户提供廉价服务的同时可以对能源使用方式进行多种选择。

2016年4月中旬，纽约推出区块链技术能源网络改革。纽约州正致力于将现有电网改造成分布式平台，促进大型公用事业公司与创新者合作，而不是竞争。为了奠定新的分布式电网基础，纽约州能源和金融部门主席考夫曼（Kauffman）颁布了改革能源愿景（Reforming the Energy Vision, REV）的政策，使纽约州现有的电网结构更清洁、低成本、有弹性。电力公司也转型成为分布式系统平台供应商（Distributed System Platform Providers, DSPPs），并将现有落后的电网系统升级，转变成个人微电网的集合体。作为REV项目的一部分，纽约州分配了4000万美元用于支持对电网去中心化感兴趣的合作伙伴。包括LO3在内的150家申请机构中，已经有83家收到10万美元的可行性研究经费。纽约州希望

尽快发布REV第二阶段的提议竞争，意见采集截止日期可能是2016年秋天。第三、四轮的获胜者分别会获得500万美元奖金，用于完成相关项目。

这个举措收到了意外的效应，为LO3提供了很好的发展环境。尽管LO3没有入选项目的第一阶段，但是却很符合第二阶段的要求；第二阶段设置了10个获奖名额，每个提供工程设计和企业计划的企业各自会获得100万美元奖金。

（四）德国电力公司RWE

2016年3月8日，德国电力公司RWE将整合以太坊区块链技术与汽车充电站服务。不同于其他德国公用事业公司，RWE最初的能源生产模式面临着监管问题。这个事实推动了RWE的革新，其中一项举措就是建立内部工作小组，评估区块链技术怎样帮助公司减少能源传输成本。公司与基于以太坊区块链的初创企业Slock.it [以太坊前首席文化官史蒂芬·蒂阿尔（Stephen Tual）创立的] 合作研发了“概念证明”机制。

RWE区块链团队领导人卡斯滕·斯托克（Carsten Stocker）谈到了一项可行的应用，利用区块链智能合约验证用户身份和管理计费过程的电力汽车充电站，通过建立无缝低廉的充电基础设施推动电力汽车使用率。这个项目的工作模型在瑞典日内瓦创新LIFT会议中首次亮相。下个阶段就是对这个模型进行电力汽车和充电站的实际测试。

相关“概念证明”机制是基于以太坊区块链的，客户身份验证和支付程序都是在充电站进行的。在这个模型下，用户同意以太坊网络智能合约后就可以与充电站互动。充电之前，用户需要在相关网络中存一笔钱，交易完成后便会退还。现有充电站与RWE模型功能的显著不同是收费方式，在RWE模型中，用户无须支付通常数小时的充电站连接耗

时费用，而只需支付充电电量费用。这个试验项目的论点是小型交易帮助用户省钱，同时电力利用率也更高。

公司接下来需要考虑的是，政府监管政策对该系统实际应用的影响，RWE已经着手这个项目。鉴于公司对政策的理解和现存基础设施，RWE强调德国是首批试验的最佳地点。区块链的应用可能给公司与用户交流方式带来转变。基于区块链技术的充电站将使客户与RWE的机器设备进行交易。真正让人兴奋的是，用户将不再与公司或个人签订合同，而是利用智能合约直接与机器签约。

区块链技术会改变RWE公司运营充电站的方式。这是公司缩减充电站搭建和运营成本的必经之路。还可以将其他创新项目融合到这个工作中，例如车辆自主运行。这个概念曾是智能合约应用的可行领域。区块链技术与公司科技创新远景规划非常契合，对公司发展至关重要。

（五）欧洲能源零售市场

欧洲委员会联合研究中心在英国分布式总账报告中，探讨了欧盟能源联合框架战略（European Commission Energy Union Framework Strategy）规定的“能源联盟”的愿景，“以人民为核心，人民能够有能源转化的所有权，能够从新技术中受益从而节省支出，参与市场的活动，并且保护弱势消费者”。然而，尽管智能电网的发展也在稳步推进中，但是能源零售市场还在等待现代化。该委员会正在启动的“新能源市场设计”将需要面对以下几个至关重要的问题：

其一，如何将成本和消费等信息适当地传达给消费者，这样他们就能够在一个完全整合的大陆能源市场中确认新机会。

其二，如何奖励积极参与者，有利于合同交换和管理，根据需求提供相应的动态价格。

其三，如何确保市场中对于住宅性能能源服务的交互操作，扩大消费者的选择，能够从自生产和自消费中获利，形成局部的微生产。

在这种情况下，分布式账本能够成为一个全新的驱动力，用以帮助能源市场进行整合发展。欧盟的联合中心正在调查以下案例中的实际应用可能性。

1.微发电的能源市场

微发电指的是消费者在住宅内或者在一个当地社区内进行发电。这个“市场”概念意味着，那些微发电产生的能源将可以在消费者和产消者（既是生产者也是消费者）之间进行交易。按传统方式，这个市场已经被产消者和能源零售商预先定义的双边协议确定。直到现在为止，发电的产消者还没有能够真正进入能源市场，这依旧是机构能源供应者特权垄断的领域，这就极大地限制了微发电对于终端用户的经济优势。分布式账本通过和智能电表系统，以及下一代电池（能够本地存储电量）结合，已经有潜力向能源市场提供产销一体的生产潜力。智能电表可以被用于注册和在分布式账本记录微发电的数据（成为“能量货币”系统的代币）。

自发电能够用于房屋内的消耗，也可以被存储在下一代电池中供以后使用，或者简单地返回到智能电池。另外，账本的分布式和通用性，使其所产生的能量可以在任何地方被赎回。例如在国外对电动汽车充电时，或者卖给出价最高的买家，这类似于股票交易市场中所提供的相似机制。

2.能源合同台账

一个消费者打算更换能源供应商时需要结束目前供应商之间的合约，再和新的能源供应商建立新的合约，并且重新访问由第三方提供的所有补充能源服务的合同条款。这些业务的复杂程度已经成为一个障

碍，阻碍了一个有竞争力的能源零售市场的形成，也会成为能源供应商和分销商需要承担的成本。消费者从一个供应商过渡到另外一个供应商，只需要在电脑和移动设备上点击几下鼠标就可以完成。同样，能源供应商和能源服务提供商将能够节省资源，无须支付更多的管理操作成本。

这些可扩展、安全且稳定的应用肯定还会有各种各样的问题。但是，从它的优势来看，是值得团队展开进一步调查的。

第六章 传统金融行业的区块链战略

一、银行的区块链战略

（一）高盛

高盛集团（Goldman Sachs）是一家国际领先的投资银行，向全球提供广泛的投资、咨询和金融服务，拥有大量的多行业客户，包括私营公司、金融企业、政府机构以及个人。高盛集团成立于1869年，是世界上历史最悠久且规模最大的投资银行之一，总部位于纽约，并在东京、伦敦和中国香港设有分部，在23个国家设有41个办事处。其所有的运作都建立在紧密一体的全球基础上，由优秀的专家为客户提供服务，同时拥有丰富的地区市场知识和国际运作能力。

1. 高盛报告

高盛在2015年12月发布的《高盛全球投资研究》报告中指出，比特币的底层技术——区块链技术已经做好准备“颠覆一切”。高盛认为区块链技术可以彻底改变传统的支付体系，可用于包括发行证券、智能合同等大量事物中。相比于传统的交易体系，区块链技术可以让交易更迅速、成本更低。

高盛非常看好区块链技术的未来应用，该行业分析师罗伯特·D·布鲁杰迪（Robert D. Boroujerdi）在报告中曾表示：这种去中心化基于密码学的解决方案去除了中间人，具有重新定义交易和多行业后端支持的

潜力。布鲁杰迪表示，一旦认识到比特币的底层技术，它便能够迎来一些削减成本的新工具，挑战那些中间人的利润池，有望让这些中心化机构变得过时。这种解决方案承诺的，不只是针对消费者的机会，同时也针对那些更想获利的企业。去除中间人意味着区块链技术能够更有效地运作，比目前的系统更可靠，且成本运行更低。它还可以减少对手的风险，具有潜力提供交易风险和成本的即时反馈。布鲁杰迪在报告中还强调了区块链技术的一些应用案例，范围从支付系统到银行的后端流程（如会计、人事、结算等）和监管文书工作，到为替代性资产做公证（如艺术品），还有投票系统或车辆登记，还可以用于提供学历证书的记录。

不过，报告中也指出了一些区块链技术存在的潜在问题。例如社区内常谈到的被限制的交易吞吐量问题，目前比特币区块链限制在了每秒进行7笔交易，这与VisaNet的核心网络支持的每秒47000笔交易相比，并不具有优势。

2.投资Circle

2015年5月前后，高盛集团与中国IDG资本（IDG Capital Partners）结成了伙伴关系，对比特币创业公司Circle Internet Financial领投5000万美元，这是一家以利用技术支持下的比特币来改良消费者支付方式的创业公司。

Circle的联合创始人计划利用比特币来进入生机勃勃的P2P支付市场，这个行业目前的领导者是Venmo等公司。Venmo是贝宝旗下的一个应用，允许用户与好友之间迅速进行转账，而且无须使用支票或银行转账等手段，不过这些汇款方式可能需要几天时间才能完成转账。

Circle近期的目标是像Venmo那样提供免费的瞬时转账服务，但该公司希望比特币能在未来允许其提供同样方便的跨境转账服务，而这是Venmo无法做到的。此外，Circle还宣布推出新的账户功能，可使用户

持有、发送和接收美元。据Circle透露，这些资金将由美国联邦存款保险公司负责投保。该公司推出的新账户功能，意味着用户可同时持有比特币和美元，选择持有美元的用户也可以同接收比特币的商家和用户进行交易，Circle会即时地将美元资金转换成比特币，反之亦然。

高盛集团首席战略投资部的董事总经理汤姆·杰索普（Tom Jessop）表示，该银行已意识到需要投资一些有望通过技术创新来改变全球市场的企业，他认为，Circle的产品愿景和卓越的管理团队在数字支付领域极具竞争力。IDG资本合伙人则表示很高兴能够参与投资，并希望帮助该公司打入中国市场，中国市场的消费者采用创新数字支付产品，其增速是非常惊人的。

Circle首席执行官杰里米·阿莱尔（Jeremy Allaire）声称，他们所提出的这种法币和数字货币混搭的模式，可以给用户带来数字货币的优势，包括即时结算、全球互用性、无交易费且高度安全，同时用户还无须使用新的货币，并重申这种混合式的模式可以让用户享受到数字货币的所有好处，且不存在风险。而Circle下一步计划是添加更多种类的货币，希望将比特币的好处与世界的几种主要货币相结合，其中包括英国（英镑）、欧洲（欧元）以及中国（人民币）。

3.SETLcoin专利

高盛在2015年11月递交了一份专利申请，是基于称为“SETLcoin”的一种全新数字货币，可以用于证券结算系统。申请日期是11月19日，其中标题是“证券结算的密码学货币”，允许点对点的参与者使用代表证券的数字货币来进行交易，并且能够进行实时结算，即交易者使用他们各自钱包中的相关资金，通过一个开放的交易，并使用所描述的技术来交易证券。SETLcoin的所有权在确认和验证后，将被实时地转移给新的所有者，这是基于点对点网络系统中的网络账本，能够确保可以准实时地执行。

根据申请的内容，SETLcoin的交易是在一个钱包软件中来实现，在一个将SETLcoin标记为某种特定证券的系统中，申请中使用IBM和谷歌的股票作为例证：一个SETLcoin的钱包或者交易可以容纳一个单种证券，如上所述，或者多个相同面额的证券（例如，1个IBM-S SETLcoin的价值相当于100 IBM Shares）。多个SETLcoin的钱包或者交易也可以容纳多个证券（例如，1个IBM-S SETLcoin和2个GOOG-S SETLcoin）。在一些实施方案中，项目内置的密码学货币（Positional Item inside Cryptographic currency, PIC）可以让某高度权威机构来进行发行（或销毁）。比如，在SETLcoin的网络中，美元可以表现为“USD”的设置代号，可以由美国财政部这样的权威机构来发行。并且，其所描述的技术可以基于其他技术（例如网络节点协议、交易规则、租赁或购买、拍卖等），还可以基于例如公司名称、市场标识、品牌、证券符号任何可选的方式来命名，也可以采用更好的格式（如长度、缩写等）。SETLcoin也是可以交易的，例如可以和其他数字货币进行交易（如Peercoin）。比如，1个IBM-S SETLcoin可以和1个或者多个“GOOG”SETLcoin进行交易，也可以和13000个USD SETLcoin、100个litecoin或5个bitcoin进行交易。

（二）摩根大通

摩根大通集团（J.P.Morgan Chase & Co, NYSE: JPM），业界称西摩或小摩，总部设在美国纽约，总资产2.5万亿美元，总存款高达1.5万亿美元，占美国存款总额的25%，分行6000多家，是美国最大的金融服务机构之一。摩根大通于2000年由大通曼哈顿银行及J.P.摩根公司合并而成，并分别收购芝加哥第一银行和贝尔斯登银行和华盛顿互惠银行，是一家跨国金融服务机构及美国最大的银行之一，业务遍及60多个国家，包括投资银行、金融交易处理、投资管理、商业金融服务、个人银行业务等。摩根大通的总部设于曼哈顿区的第一大通曼哈顿广场

（One Chase Manhattan Plaza），部分银行业务则转移到得克萨斯州休斯敦的摩根大通大厦（J.P.Morgan Chase Tower）。

摩根大通CEO杰米·戴蒙（Jamie Dimon）非常不看好比特币。他曾经公开表示，比特币不受监管的状况不会发生，没有政府会长期对比特币忍气吞声。现在比特币规模还较小，许多参议员和众议员会表示支持硅谷创新。但是事实上，没有货币能避开政府监管。但是他也承认，区块链技术让比特币成为可能，并可能改变游戏规则。据J.P.摩根内部人士透露，其内部备忘录显示，由于投资者想要确认他们在技术上进行的90亿美元投资，能否在2016年继续保持，所以，区块链、大数据和机器人这样的下一代技术，将会是J.P.摩根今后投资的重点。工作团队正被催促发展市场主导的平台，但没有透露具体的细节。

作为R3联盟的创始银行的一员，J.P.摩根已经帮助尝试将区块链带向主流。R3是召集银行业来开发银行清算结算标准和使用区块链案例的联盟。并且在2015年12月，软件非营利组织The Linux Foundation也“宣布共同努力发展流行的区块链技术”，其中也包括J.P.摩根。

戴蒙说“硅谷来了”，如果银行再不更新他们的游戏，技术企业将会接收银行业的生意。他表示，成百上千的初创企业拥有大量的大脑和资金，正在致力于开发传统银行业的替代品。目前看到的大部分都是在贷款业务，这个领域公司可以很快地借钱给个人和小企业，这些实体相信运用大数据可以有效地促进信用担保。他们非常善于减少“痛点”，使他们可以在几分钟之内贷款，而这可能会花费银行几周的时间。摩根大通将会更加努力地使自己的服务像他们一样更加顺畅和有竞争力，也完全乐意在合适的领域合作。同时，他们极其详细地分析了所有的竞争者，了解正在做什么，并据此制定摩根的战略。

戴蒙的警告和J.P.摩根对区块链、大数据和机器人的推进，最大的原因应该就是银行也已经感受到来自技术企业的压力。

（三）瑞银集团

瑞银集团（UBS）是1998年由瑞士联合银行及瑞士银行集团合并而成的，是一个多元化的全球金融服务公司，在瑞士巴塞尔及苏黎世设有总部，2001年底总资产1.18万亿瑞士法郎，资产负债表外管理资产超过2.0万亿瑞士法郎，2002年净利润35亿瑞士法郎。瑞银集团是世界第二大的私人财富资产管理者，以资本及盈利能力也是欧洲第二大银行。其中，瑞士银行共设有96个分行，遍布全美国及50多个国家，全世界的雇员大约共有49000名。

1.对于比特币的态度

早在2014年3月，瑞银集团就已经开始着手研究比特币等数字货币，并且发布了一份比特币报告。报告指出，从技术上来说，比特币的确提供了一种革命性的全新支付系统。比特币已经作为国际转账的一种廉价形式——该市场具有极大的潜力。原则上来说，金融机构和现有的反洗钱系统（如银行）可以采用类似于比特币的技术，在终端用户间构成安全和便捷的转账手段。但是瑞银也明确指出，比特币如果要作为一个真正的货币，将面临经济、技术和监管的挑战。投机驱动的波动性阻止了比特币成为一个稳定的存储价值或者单位账户，其半固定的供给加剧了波动和通缩。作为交换手段，它已经为相对较少的交易消耗了大量的计算资源。比特币也存在一些监管真空，而且在一些司法管辖区中，它是被禁止或被限制的（如在俄罗斯、中国），破坏了人们对比特币的信任感。

就像高盛一样，瑞银更看好比特币的基本概念：区块链技术。通过给用户直接控制自己资金和使用加密方式的私钥，比特币式的系统能增强安全性，降低成本。原则上来说，这种支付系统可能会成熟，并被第三方所使用，甚至在处理存款上挑战银行（可能仅仅是在线业务上），因此有可能对现有的银行构成威胁。

2.区块链实验室

瑞银一直是对数据区块链技术最开放的大型银行之一，并在伦敦开设了一个名为“Crypto 2.0”的技术研究实验室，该实验室将研究如何在金融业务中利用区块链技术。

该实验室于2015年4月正式开放，在伦敦最新建成的39层标志性建筑金丝雀码头大厦中，拥有能容纳12个办公桌的办公室。瑞银集团称，实验室将汇集银行业和金融业的专家。实验室的成员和特邀专家将研究区块链是如何工作的，如何利用区块链技术完成大规模的金融交易，同时让交易变得更有效率、成本更低。实验室将努力开发相关技术用以解决一些全行业都面临的共同问题，例如如何管理和分析海量数据，以及如何更好地评估投资风险等。

越来越多的金融机构对比特币背后的区块链技术产生兴趣，而瑞银集团是第一家公布将正式研究区块链技术的金融公司。这个决定将让瑞银集团与伦敦的金融创新前沿技术联系得更为紧密，为瑞银集团的发展提供外部创新动力。瑞银称其已经开发出数据区块链技术20多种用途，正在对一些最佳用途进行孵化。其中一项实验就是通过所谓“智能合约”来开发出一种“智能债券”，包括利用数据区块链技术来重建债券的发行、利率计算、票息支付和到期过程。

在2014年10月接受记者采访的时候，瑞银集团首席信息官奥利弗·巴斯曼（Oliver Bussmann）就表示，区块链技术具有强大的潜力，它不仅会改变现有的支付方式，它还会改变整个金融交易结算的方式。他称这项技术具有颠覆现有金融服务方式的潜力，可能会触发大规模的银行业简化交易流程和降低交易成本的革命。对于金融科技实验室，巴斯曼认为，只有在银行家、创新者和投资者之间营造一种开放和谐的环境，各方才能更好地合作，为金融行业创造出真正有价值的技术。

3.投资回报率

对于全球金融机构而言这是一个分水岭时刻：世界上最有钱的投资银行之一，将它们的财富以及公众形象投放到区块链技术之上。从2013年开始，越来越多的银行再次开始与金融科技创业者们进行互动，它们希望能够和金融科技一起发展前进，而不是被这些威胁到它们的创新技术所淘汰。

瑞银集团“区块链创新实验室”前任负责人亚历克斯·巴特林（Alex Batlin）认为，虽然例如P2P借贷以及众筹平台这类金融技术，仍处于上升阶段，但区块链技术，才是瑞银集团最大的威胁或者说是机会，因为它可能是目前汇合最多东西的技术以及商业之一。而巴特林的主要任务就是为银行的股东们从这些日新月异的变化中找到一种能够获利的方式。

通常情况下，对于一个新的想法，瑞银集团在其承诺进一步探索之前，都能够评估其投资回报率（ROI）。然而，由于区块链技术实在太新，而且变化过快，该银行的常规对策显然已不再适用了。在这种情况下，想要计算出投资回报率，你就必须花很多的钱……你需要一个ROI中的ROI。在巴特林看来，这就是一个鸡与蛋的关系问题。而瑞银集团所创建的这支团队，用他的话来描述就是：这是一支由开发者、业务分析师以及欧洲最大Fintech加速器Level 39（欧洲最大的金融技术类公司孵化器）的项目经理组成的敏捷小团队。团队有很多的时间就是在会议室里进行头脑风暴，大家一起想新的商业模式，然后进行测试。他们所进行的测试，与概念证明是不同的，因为他们没有一个概念，而只是说，这里有一个假设，然后大家来弄清楚它能否行得通。这样的系统具有潜力去除市场的复杂性，并降低参与成本。

然而，随着越来越多的区块链争夺市场份额，公司们可能会遇到另一个问题——交互可操作性的减少。相比于多个闭源系统，例如MSN（微软网络服务）以及AOL（美国在线），巴特林心中真正的成本节约，是来自一个共同的标准，这就好比是互联网，作为一个多资产

链，人们可以在同一个平台上，进行证券交易、衍生品交易以及现金交易。

英国伦敦正迅速成为金融与技术交叉点的枢纽。该国2015年的Fintech企业投资，占据了欧洲市场42%的份额，而相关的企业员工更是超过了13.5万，其中的大多数都在首都伦敦。除了其成熟的Fintech生态系统，英国政府对于数字货币豁达的监管态度，对于这家瑞士银行的项目来说，也具有很强的吸引力。

在金丝雀码头的Level 39中心，这里的Fintech与政府之间有着紧密的联系，金融市场金融行为监管局（FCA）就在马路的对面，而英国央行，也是Level 39中心的一个常客。人们很乐意来这里开会，并非是因为瑞银集团，而是因为Level 39。虽然在生态系统中的一些创业公司以及风险投资者们，包括Index的奥菲利娅·布朗（Ophelia Brown），都在严厉指责银行拒绝为比特币初创公司提供银行账户服务，但巴特林则有不同的看法。他认为全球数以千计的客户，依靠他们这类专业人士给予意见、专业知识以及机会，所以他们自然要更谨慎一些，拿客户进行冒险是不负责任的。而有些问题，让初创公司来解决，又可能有些过于昂贵。比如，一个12人的团队，当然可以完成很棒的东西，但有一些挑战需要资源来克服，而例如瑞银集团这样的公司可以为此提供帮助，成为这个新世界有价值的合作伙伴，所以，大公司与初创公司之间的合作关系，可以进行得非常融洽，因为双方之间可以进行互补。

4.开发数字货币

据《华尔街日报》（The Wall Street Journal）报道，瑞银正致力于开发一种数字货币原型，希望银行和金融机构可在未来使用这种货币作为主流金融市场交易的结算手段。

但瑞银正在开发的这种“结算币”（settlement coin），与数字货币比

代币有所不同，这种货币将与真实世界的货币和央行账户联系在一起。数字货币将被用于对机构金融平台上的交易提供支持，这些平台基于区块链技术而被建立起来，类似于比特币赖以完成交易的分布式总账。

举例来说，瑞银可能会拥有自己基于区块链技术的平台以发行债券，而另一家银行则可能拥有一个基于区块链技术的股票交易平台，但这两个平台都可使用同样的“结算币”来进行结算。

瑞银正在与伦敦创业公司Clearmatics联手开发这种数字货币，这家公司已经开发出了一种基于区块链技术的软件，可以对金融交易进行清算和结算。瑞银高管表示，并不计划单靠自己发行这种数字货币，而是希望与其他市场参与者——如资产管理公司、监管机构以及票据交换所和交易所等市场结构提供者——合作来打造一种全行业产品。

瑞银的电子商务商业主管海德·杰弗里（Hyder Jaffrey）表示，该行已经与一些潜在的合作伙伴进行了接触，但并未透露具体有哪些机构。该行及其他金融机构认为，如果区块链技术能得到广泛采用，那么就能让金融机构在短短几秒钟时间里完成交易结算，而不是像现在这样需要两三天才能完成。

瑞银的这个项目现在还处在概念阶段，由该行旗下伦敦的区块链实验室负责。该实验室的主管巴特林和瑞银的首席信息官奥利弗·巴斯曼称，这种数字货币可能是基于区块链技术的平台，在主流金融市场上得到广泛采用的第一块“积木”。

（四）德意志银行

从2014年开始，德意志银行就开始研究区块链应用，后来加入了多个银行组成的联盟，来共同探索区块链技术。而他们目前获得最重要的结论就是，该技术“将会改变许多金融行业的商业模式”，并且在未来可

以看到许多不同的形态。

德银《流动》（**Flow**）杂志2015年10月刊指出，该机构称其已经发掘通过一个“创新实验室”来研究数据区块链技术的潜力。德银指出，数据区块链技术的应用将面临“巨大的法律和监管障碍”，但承认它可能对当前银行业产生巨大颠覆效应。

2015年12月初，德意志银行进行了基于区块链技术的可编程债券实验后，认为区块链技术将会在未来十年内逐渐成为主流。

尽管拒绝透露和该银行一起参与实验的两家供应商，但是德意志银行表示价值证明（**Proof-of-Vall, PoV**）测试已经成功完成。公司债券是测试基于区块链资产的理想标的物，德意志银行将会用它来测试资产的完整生命周期（发行、票面利率、赎回），这就是为什么德意志银行选择了它。在这个阶段，作为本行首个商业化的产品，德意志银行将不会追求实现智能合约。

根据银行的说法，测试结果既获得了令人信服的答案，也发现了一些全新的问题，将在未来对技术进行更进一步的探索。

德意志银行最近的测试重点是可编程债券，因为该机构要探索“智能合约的完整生命周期概念”。这将会涉及对基于不同区块链的案例进行同步调查。

目前测试的结果是，区块链技术实现了所有他们在**PoV**测试中设置的规模目标，需要更进一步充分测试这些用例的可扩展性和稳定性。

德意志银行表示，他们希望看到在未来两年的时间里，更多基于区块链的商业化产品投入到市场中。将会有许多有访问限制的私有链出现.....而在他们之间实现数据移动会变得非常重要。

（五）桑坦德银行

桑坦德集团成立于1857年，总部位于西班牙北部的桑坦德。桑坦德是西班牙和拉丁美洲主要的金融集团，拥有150年的历史并且在40多个国家设立了分支机构，是欧元区排名第一的银行，同时也是全球市值排名位居前列的银行之一。

1. 预测报告和态度

根据桑坦德银行在2015年发布的一份预测报告中称，到2022年，它每年可能至多为银行省去200亿美元的费用，通过使用某些非比特币类型的分布式总账和区块链技术，每年可以为银行节省近200亿美元。桑坦德风险投资基金Oliver Wyman和Anthemis Group表示，到2022年区块链技术每年可以降低15亿~20亿美元的基础设施成本。桑坦德总经理马利亚诺·贝尔金（Mariano Belinky）表示，银行不应该专注于数字货币本身，其底层协议才是最强大的。相信在未来，该技术将会更多地被采用。

福拉（Faura）是桑坦德银行研究开发方面的领军人物。同时，他也致力于银行的M&A（企业并购）事项及金融投资。他认为技术和资金同样重要。他以前是SIDSA（西班牙半导体公司）的芯片设计师，后来到麦肯锡公司当顾问，加入到西班牙、欧洲及拉丁美洲的金融机构中。2007年，福拉来到了桑坦德银行，致力于消费金融、投资银行学、技术运算等方面。作为桑坦德在创新方面的领军人物，福拉专攻数字货币、手机支付及电子商务。虽然桑坦德还不确定是否使用区块链技术，但是福拉表示银行内部最近正在进行区块链技术的研究，他认为区块链技术在国际支付上很有潜力。

在2015年11月13日伦敦举办的英国央行公开论坛上，瑞士投资银行和西班牙最大的银行桑坦德银行讨论了区块链技术。桑坦德创新部的全

球主管乔·玛丽·福斯特（Jose Maria Fuster）在小组讨论中评论了区块链技术对于金融行业的潜力，旨在阐述金融创新和技术将如何为经济提供支持。他说区块链技术非常符合比特币的理念……这种技术允许人们在货币转移、货币存储的基础设施上创建出一个全新的空间，并且在其中建立智能合约来完成许多复杂的行为，从而在根本上改变目前金融业的面貌。但这并不意味着改变就会在明天发生。尽管在小组讨论中大多数人并没有提及比特币和区块链技术，但福斯特还是敦促他的同行们不要忽视创新，创新是一个全新的概念，也是一种战略工具，如果你不创新，就有人会取代你的商业模式，这对于金融业而言有着非常广泛的意义。

2.区块链竞赛

桑坦德创新风投（Santander InnoVentures）是桑坦德银行的互联网金融投资基金，在2014年设立1亿美元资金，专门用于支付、市场借贷、电子投资咨询、客户和风险分析，以及提供数字金融服务。

2015年11月，桑坦德创新风投宣布启动一个全球区块链竞赛，寻求对那些采用分布式总账技术的早期初创企业提供支持。这个来自西班牙大银行的1亿美元的风险投资公司——最近参与了Ripple的3200万美元的投资——这次将会为胜利者提供15000美元的现金奖励，以及提供专业的技术和企业专家。

桑坦德创新风投的管理合伙人，马里亚诺·别林基（Mariano Belinky）表示，分布式总账技术，将会让客户、银行和企业围绕着它带来极大价值。这个竞赛将会激励和加速互联网金融创业企业的进程。桑坦德创新风投已经和初创代理OneVest结成伙伴关系，将会为天使投资者提供辅导和指导。

（六）巴克莱银行

巴克莱银行（Barclays Bank），是全球规模最大的银行及金融机构之一，总部设于英国伦敦。巴克莱银行于1690年成立，是英国最古老的银行，具有逾300年历史，是全世界第一家拥有ATM机的银行，并于1966年发行了全英第一张信用卡，于1987年发行了全英第一张借记卡。截至2013年，全球雇员达到140000人。截至2012年，总资产高达1.49万亿英镑，成为全球第七大银行，是位于汇丰银行（HSBC）之后的英国第二大银行。巴克莱银行在全球50多个国家经营业务，在英国设有2100多家分行。

1.接受比特币捐款

巴克莱银行在2015年5月表示，比特币在多方面创造了一种“比当前支付体系更优雅的解决方案”，但在多个领域依然“存在不足”。该行在报告中预计未来将会有更多数字货币问世，而且可以弥补第一代比特币的缺陷。该行首席设计和数字官德里克·怀特（Derek White）明确表示，巴克莱允许比特币交易所帮助慈善机构接受比特币，并透露了一些关于和比特币交易所合伙的细节。

巴克莱银行也在不断研究和扩大比特币区块链技术，计划让客户们通过与比特币交易所相互合作，来使用数字货币进行慈善捐款。这表明，巴克莱银行并不想被时代抛弃，同时他们也看到了比特币降低基础设施成本的潜力。该银行已经在伦敦建立了两个比特币实验室，并且和一些初创公司进行合作。巴克莱银行还使用了伦敦东区白教堂内的一个翻新仓库来举办比特币爱好者之间的聚会，这样做的目的在于加强对比特币和资料库感兴趣的初创企业、学术界、政府的相互合作及彼此联系。

比特币区块链记录了所有比特币交易，并不是只有巴克莱银行看到

了其中的潜质，瑞士银行也想要在这方面研究一番。前巴克莱CEO安东尼·詹金斯（Anthony Jenkins）在2015年或更早的时候，曾经发出警告，认为银行正在面临“Uber时代”，这将会让银行削减掉50%的职员。一些迹象表明，11个大银行在2015年已经削减了10%的职员。

2.巴克莱加速器

2015年10月24日，纽约的巴克莱加速器（Barclays Accelerator）演示日上，有11家公司展示了它们创新的互联网金融方案。在其中有8家企业已经和银行签订了合同。在演示后的13周内，将会有密集的网络搭建、指导和发展活动。

巴克莱加速器计划是作为Tech Stars Global（隶属于TechStars公司）网络提供合作的，主要的内容包括为金融科技初创公司提供辅导和机会，可以让创业企业来接触行业专家，以及有影响力和潜在的客户。该项目覆盖了互联网金融的大部分领域，包括从网络安全到人工智能，从财富管理到投资银行，还有大数据和数字货币。接下来13周课程将会在伦敦进行，直到2016年1月。巴克莱宣布，接下来的两次的巴克莱加速器机会将会是2016年3月，在特拉维夫和开普敦进行。

2015年6月，10家公司参加了巴克莱的伦敦12周加速器计划，有7家公司和银行获得了“探索性机会”。巴克莱银行和一家瑞典企业Safello签订了协议，该公司参与了伦敦的加速器计划，研究区块链如何在传统金融领域使用。

巴克莱首席设计和数字官德里克·怀特表示，在巴克莱正在拥抱数字革命、开拓创新，在初期，巴克莱会帮助他们来构建发展规划，和这些初创企业共同打造金融服务的未来。还将领导行业新技术的开拓，这将是极为重要的，帮助巴克莱实现“去银行化”的雄心。

2015年3月，在伦敦举办的摩根士丹利欧洲金融会议上，前巴克莱

银行的CEO安东尼·詹金斯警告说，银行业还没有遇到技术的“全面破坏性力量”——但它一定会遇到。他阐述说，金融机构的担忧正在快速增长，更加低成本的系统将会在未来几年中抢走他们的消费者和企业客户。TechStars的董事总经理珍妮·菲尔丁（Jenny Fielding）表示，成为纽约市快速发展中的互联网金融系统的一部分是非常令人惊讶的，并且在产业转型中发挥积极作用。11个初创公司分别对应不同的金融服务类型，进一步证明了在这个巨大的市场有不同的机会。对于这些高速增长中的初创企业而言，与巴克莱银行一起工作，将证明巴克莱的确是一个强有力的合作伙伴，巴克莱很高兴能够在世界范围内推出更多的互联网金融方案。

巴克莱选择了两个特别专注于区块链技术的互联网金融公司，巴克莱的金融犯罪和交易监视小组，它们将会使用Chainalysis工具来深入实时地分析区块链交易数据，以获得在区块链上的客户金融交易信息。Chainalysis是一家总部位于瑞士的企业，该企业使用合规的手段来对区块链进行实时分析，并且以此来为金融机构提供服务。Wave——另一家开发了完全去中心化点对点网络的企业，用以连接所有的相关运营商，这些运营商可能包括诸如银行、代理、贸易商，以及国际贸易供应链中的任何一方，它们也是用基于区块链的工具，来帮助那些与巴克莱企业银行（Barclays' Corporate Bank）在供应链上进行合作的相关商业客户降低成本。

很明显，比特币正在逐渐走向主流和合规化，因此类似于Chainalysis这样的服务会被需要，但是这样的服务正在遭受比特币社区众多人的反对，一份已经泄露的Chainalysis发展路线图被公布在Reddit社区，引发不少愤怒和有敌意的评论。

2015年8月，据称巴克莱银行将成为首家帮助某些它挑选的客户——英国的慈善团体——用自己的银行直接接受比特币的机构，这开创了历史先河。可以预期的是，在主动将注意力放在慈善事业之后，巴克

莱银行考虑逐步让普通商业客户和长期客户来接受比特币支付。在此背景下，Chainalysis系统可以让巴克莱银行能够完全使用合规的应用来分辨出客户的优劣程度。

3.区块链实验室

2015年9月，英国银行业巨头巴克莱已经在伦敦运营了两家工作站，或称“实验室”，专注于区块链创新技术。这两家机构位于诺丁山和伦敦的老街区，靠近伦敦金融城。它们将致力于比特币和区块链领域、业务和开发，大约有75个工作人员在进行探寻比特币和其区块链的工作。

（七）美国银行

1.申请大量专利

美国银行（Bank of America）正在试图通过不断地申请区块链技术相关的专利，谋求在该技术领域抢占先机，并尝试通过申请该技术的某些用例专利。美国银行运营和技术办公室主管，凯瑟琳·贝松

（Catherine Bessant）2016年1月的达沃斯论坛上表示，美国银行已经申请了区块链技术相关的15项专利，目前正在起草的另外25项专利将会在2016年提交给美国专利和商标局（USPTO）。

她指出，区块链技术非常有趣，但对于美国银行而言需要取得一种平衡，既不想坐着傻等，最后变成灭绝的尼安德特人，也不想马上把它投入到商业应用中，毕竟截至目前该技术在商业中应用的前景还不是太明晰，尽管其极具吸引力。

美国银行正在试图站在行业的最前沿，在该领域已经有了15项专利，有许多人或许会对于美国银行正谋求在区块链技术和数字货币获得

更多专利感到惊讶。但是他们知道，在了解其真正的商业应用前景之前，进行知识产权的储备对我们来说非常重要。

在2015年12月，美国专利和商标局公布了美国银行申请的10项专利，美国专利和商标局一般在他们申请专利18个月后进行信息公布。但信息显示，美国银行申请和正在申请的专利数量显然要高得多。

美国银行申请的专利包括“数字货币的风险检测系统”“可疑用户警报系统”等，这些专利还没有被授予。区块链技术要成为银行业的主流可能还需要一点时间。但目前，多家银行正在积极探索这一领域。

2.区块链贸易融资试验

美国银行在2016年3月宣布，银行正针对贸易融资开发一种基于区块链技术的试验。此举是近期跨国银行机构将自身定位于区块链技术早期采纳商的最新例证。2015年12月下旬，美国银行披露已提交一系列与该行业相关的新专利。就在2015年11月，该银行发布新闻宣布与财团新秀R3展开战略合作。

美国银行认为区块链有望取代在全球贸易领域居主导地位的手工流程。

美国银行全球交易服务创新部负责人杰森·蒂德（Jason Tiede）向媒体表示，他们正在贸易融资领域进行试点测验。贸易融资以往过于依赖手工、纸笔流程，这个试验能够体现在分布式总账上数字化资产的价值，是有趣的用例。值得注意的是，该项目是美国银行与另一家不愿透露姓名的银行联合开展的。蒂德说，该试验应该在2016年春季之前完成。

公告显示，美国银行已加入渣打银行与新加坡发展银行（DBS）之列，成为积极寻求在贸易金融领域采用区块链技术的大型银行。

二、金融和IT巨头的区块链战略

（一）DTCC

1.关于DTCC

美国存管信托和结算公司（Depository Trust & Clearing Corporation, DTCC）及其子公司通过全球各地的多个经营性设施和数据中心，使全球数千家机构的金融交易处理实现自动化、集中化和标准化。DTCC拥有近40年的经验，是全球金融服务行业首屈一指的交易后市场基础设施，可简化股票、公司和市政债券、政府和抵押支持证券、衍生品、货币市场工具、银团贷款、共同基金、另类投资产品和保险交易的清算、结算、资产服务、全球数据管理和信息服务的复杂性。2011年，DTCC处理了总价值约为1700万亿美元的证券交易，其储存库为122个国家和地区发行的价值39.5万亿美元的证券提供托管和资产服务。DTCC的全球场外衍生品交易资料储存库记录了总名义价值超过500万亿美元的全球交易（包含多个资产类别）。

DTCC全球交易资料储存库打算将其业务拓展至新加坡，建立一个总部位于亚洲的全球数据中心，以确保监管机构可以无缝访问用于场外衍生品市场系统性风险缓释的数据。DTCC致力于帮助全球客户和监管机构建立强大的经营性基础设施，这种设施可以提高场外衍生品市场的透明度并降低其风险。DTCC的全球交易资料储存库服务发挥了重要作用，帮助全球的公共和监督管理机构全面了解有关市场参与者从事场外衍生品交易的风险，以及更好地了解这个复杂市场的规模和范围。DTCC的这个计划和策略旨在确保全球交易资料储存库能够为全球的监管机构提供及时和同等的交易信息。此外，随着全球监管机构制定新的

规则（要求向交易资料储存库报告所有衍生品交易和其他场外交易），该数据中心将帮助市场参与者满足当前和未来的监管要求。

DTCC还在荷兰建立了一个新的欧洲数据中心，以支持全球交易资料储存库。新加坡的数据中心预计将于2012年末建成并投入运营。DTCC还打算在新加坡为全球交易资料储存库注册所有五个资产类别，并且将与新加坡所有地区监管机构和业界紧密合作，在DTCC将业务拓展至亚洲的过程中使全球交易资料储存库获得更高的认可度。DTCC从全球场外衍生品行业获得了极具竞争力的储存库建造合同，这些储存库旨在向监管机构报告有关全球场外信用、股票、利率、商品和外汇衍生品交易的信息。信用、股票、利率和商品衍生品的全球储存库已经投入运营，而外汇衍生品的储存库也将投入运营。

DTCC为场外信用衍生品开发了最初被称为TIW的全球首个交易资料储存库。如今TIW储存着超过98%的全球所有场外信用衍生品的交易信息。经过一个竞争过程之后，DTCC随后获得了行业批准，为股票、利率、商品和外汇场外市场开发全球交易资料储存库服务。为了支持这些市场，DTCC还开发了一个基于网络的独立监管门户网站，该网站基于自愿报告协议和监督管理机构授权，让全球各地的监管机构可以获得有关信用衍生品交易的准实时信息。后来该门户网站经过拓展覆盖了场外股票衍生品和利率衍生品，并且还将用于商品和外汇交易报告。目前全球约有40家监管机构使用该门户网站来监控衍生品。

2. 《拥抱颠覆》白皮书

2016年1月，DTCC发表了一篇白皮书，呼吁全行业开展协作，利用分布式总账技术改造传统封闭复杂的金融业结构，使其现代化、组织化和简单化，该技术还可用以解决目前交易后过程局限性的问题。

DTCC的总裁兼首席执行官迈克·博德松（Mike Bodson）表示，金融业面临一个旷世难逢的机遇，抓住这次机遇，就能使金融市场结构现

代化，解决长期存在的可操作性挑战。为了以负责任的方式挖掘分布式总账技术的潜力，避免多个无关联的封闭式方案，整个行业必须通力合作。

白皮书的名称是《拥抱颠覆：开发分布式总账的潜力，改善交易后的环境》。该白皮书指出，尽管目前的金融市场结构可以提供稳定的、可靠的、可追溯记录，但金融市场结构仍非常复杂、封闭，无法进行一年365天24小时的处理。DTCC认为一系列资产配上完整的，可追溯的交易记录的分布式总账才是安全的，而这些记录只对信托方开发，如此将会大大改善交易，同时降低风险和交易后成本。

依据DTCC的研究和分析，DTCC建议开发目标机遇，在某些确定的领域改善既有结构，这些确定的领域是：自动化受到限制或不存在，与既有处理过程相比，新技术提供了明显的优势。需要开发的机遇包括：主数据管理、资产/债券的发行和服务、确认资产交易、交易/合同确认、记录和配比复杂的资产类型，目前对这种资产没有有效的解决办法、净额清算、抵押品管理，以及长期结算。

但是，白皮书提醒，分布式总账技术还不够成熟，且未被证实，目前该技术还有内生规模化限制，缺少下层结构，所以不能完全整合到既有金融市场环境之中。因此，该技术可能不会是每个问题的解决办法，但DTCC可以将其看作是一个替代方案，博德松通过标准化的工作流程和拓展云技术的使用来降低成本降低和风险降低的概率。

另外，白皮书指出，迄今为止，各方并没有开始合作进行研究，因此，行业面临重复过去失败经验的风险，产生无数基于不同标准的，经过重大妥协的复杂的封闭解决方案。最符合逻辑的方法是：既有的经过监管的具有公信力的中央权威机构在帮助技术发展中扮演领导角色，为分布式总账技术的应用引入标准、管理和技术。此外，认为这些机构应与全行业展开合作，以确保新机遇、新技术能为交易后过程带来益处，与长降低风险这个长远目标相一致，提高效率，为市场参与者降低成

本。

博德松认为，目前很多公司私下里的测试方法是利用一种使用共识协议以提高透明度的技术。这种方法可能会导致交易后的环境没有发生改变，很多公司仍会面临整合与和解的问题。作为一家存在了超过40年的金融市场公司，DTCC是唯一一家能够领导研究力量，探索分布式总账技术如何能简化或取代现有交易后系统的公司。

DTCC给出了承诺，推动交易后领域分布式总账技术。作为此承诺的一部分，DTCC付诸实际行动，他们为DAH注入了一笔资金。DAH是一家为金融服务领域开发分布式总账技术的公司，博德松将成为该公司的董事会成员之一。DTCC通过这笔资金，促进了全行业的合作，帮助引进标准，企业管理和技术为分布式总账的应用提供了支持。

3.教育和实验

2015年DTCC在证券交易了1.6万亿美元，如果停止金融交易链，DTCC就会有巨大损失。所以DTCC过去几个月一直努力把自己放在大范围实验的中心，和其他公司一样也在开展区块链技术。

DTCC不仅没有与比特币分布式总账技术对抗，相反接受了这个新工具，同时使用此技术定义了该行业的未来架构，即使这意味着改变公司的商业模式。

DTCC首席技术架构师罗伯特·帕拉特尼克（Robert Palatnick）表示，DTCC的部分责任是帮助行业创新，如何使用分布式总账解决行业问题。如果这意味着DTCC需要改变商业模式，那就是这个行业需要DTCC做的。

DTCC向用户收取账户费但不包括临时月租费和手续费。每年证券交易总额超过1万亿美元，在最近的年度报告中，即使少量手续费叠加

起来平均也有1.4万亿美元。但是理论上，区块链的潜力能让企业消费者自己进行交易后找到的解决方案来改变。

为了普及区块链颠覆性潜力，DTCC在2015年12月加入了非营利Linux基金会的超级账本项目，这是一个推动区块链技术的合作项目。利用这层合作关系，DTCC可以在创立公司管理，在技术制定标准的过程中起关键作用，并确保技术是开源的。DTCC系统总监帕尔达·维士努莫拉卡拉（Pardha Vishnumolakala）成为该项目技术指导委员会的一员。虽然现在仍然处于初级阶段，超级账本主要使用区块链技术来提供开源金融解决方案。帕拉特尼克说，但这只是公司推进计划的开始。

帕拉特尼克并没有提及DTCC正在与哪个具体的银行和机构联系，但是他表示正在做实验把区块链技术整合成一个大的资料库基础建设，努力把过往交易识别做到和Google搜索一样简单。

频繁的实验在DTCC的“闲置地区”中进行，平均结算时间大约三天，但是需要数月来关闭结算。在2016年3月，500位DTCC客户参加的圆桌会议中，公司讨论了在2017年9月5日前把结算时间缩短到两天的方案。

帕拉特尼克表示，DTCC（由几个使用它的银行组成的私有公司）没有使用单一区块链，但使用的是不同的分类账本，这个分类账本是每个用自己的方式去中心化并从属于公司的贸易后服务。

确实，区块链的潜在颠覆性影响在全球证券行业促成了一些有趣甚至令人惊讶的合作。虽然DTCC资助的实际实验内容仍然处于保密状态，但那是当数字资产的另一位投资者ICAP宣布，已经完成了针对交易后流程的内部区块链测试，也能够得到一些关于正在进行的工作的暗示。

4.阻力和生存

尽管所有的研究都是关于区块链技术如何与清结算贸易进行结合，但是这样的公司模式被分布式总账所影响的联合创始人认为，DTCC的努力恐怕是无用的。

Firm 58主要是管理纽约证券交易所和美国股票和期权交易所的交易费，其首席技术官吉姆·马伦（Jim Mullen）就表示，无论他们准备做些什么，都需要认真审视这个技术，本质上，他们需要记住区块链的精髓就是，有了区块链，他们将变得不再重要。

马伦的公司通过分析客户的数据帮助客户，他认为还没有一种方法能给DTCC提供区块链技术，公司采用分布式总账技术，这样就不再需要交易商了，但是仍然需要一个中心化的有经验的权威机构来资助、托管和维护去中心化总账。

事实上，DTCC曾经就有一段在颠覆性技术下生存发展的历史。

公司是1999年用现在的名字而成立的，是由存管信托公司（DTC）和国家信托清算公司（NSCC）合并而来，两家公司都是在1968年华尔街文书作业危机（Paperwork Crisis，也称证券洪流危机）时成立的。

那时候，老式的文本交易文件已经跟不上加速变化的汇率，机构使用新技术使过程数字化。现在在139个国家中，DTCC每天处理超过1亿美元的数字交易。尽管有这样的经验，但帕拉特尼克承认他接到的每个从供应商（做区块链实验）打来的电话都能让他更了解这项技术如何影响公司账本底线。

帕拉特尼克最终表示，他非常希望能够按快进键来看一年后事情会变成什么样子，这样他就可以集中所有的资源来做这件事。

博德松还承诺在纽约进行区块链实验，他把DTCC在未来区块链改变商业扮演的角色，定位为一个解决过于拥挤的环境的方法。他相信，

传统的信托机构应该扮演一个领导者角色，来支持分布式总账的实施。

博德松假设这样的参与可以帮助提高效率并且减少成本，进而帮助行业处理大量的挑战，讨论新技术的存在问题。围绕分布式总账的可扩展性的持续性问题，博德松引用了围绕比特币的讨论，某些网络特征是否应该被改变，来允许每次进行更多交易。他注意到最近比特币把交易验证时间提高到43分钟，认为这是区块链运用到更广泛领域的标志，可能正努力调节DTCC使用的现存技术量。

最近的一个区块链测试成功地将分布式总账技术应用于信用违约掉期，掉期市场的合同金额高达百万亿美元。

5.百年难得一见的机遇

2016年4月，博德松在最近一封致股东书中，将2015年称作“区块链技术成为主流”的一年。他透露了DTCC首席技术架构师帕拉特尼克的意见，即区块链将会从“炒作”可以转变成现实。

博德松指出，这是百年难得一见的机遇，可以实现交易后环境的现代化，因此需要联合起来确保第一步行动的正确性。

这个声明回应了ASX首席执行官埃尔默·马克·库珀（Elmer Funke Kupper）的观点，他说区块链技术是“20年难得一见的机遇，我们可以拥抱更低成本和更高效率的创新”。

帕拉特尼克在金融服务领域从业的30年间，从未见过围绕区块链技术的这种狂热。帕拉特尼克说，尽管区块链技术的潜能和机遇让人兴奋，但还是存在一定的限制。

博德松引用帕拉特尼克的话，指出分布式总账仍不成熟，还缺乏证明。他们本质上有规模限制，也缺乏无缝整合到现有金融市场环境的底层基础设施，并且帕拉特尼克认为短期内分布式总账技术也不会被广泛

采用。

大型银行和服务供应商之间的区块链狂热最终会变成现实，一系列的技术开发热潮会创造“分布式总账的孤立迷宫”。因此帕拉特尼克呼吁全行业的广泛合作，进行金融业的现有核心流程的开发和重新架构，用分布式总账替代它们。

（二）Visa

2015年11月，Visa欧洲宣布使用区块链技术来进行汇款。不过，尽管目前有许多的同行正在寻求构建封闭或者私有的账本，Visa欧洲联合实验室（Visa Europe Collab）创新合伙人乔恩·唐宁（Jon Downing）已经明确表示，目前他们测试的项目使用的是运行中的比特币区块链，进行支付的“概念证明”，并解释说，在测试环境中，资金通过区块链进行跨境发送，并且通过Visa设备进行接收。可以用法币发送一笔支付交易，然后通过M-Pesa（肯尼亚移动货币服务）来接收，但是通过利用某个区块链供应商，能够完成汇款。

这次测试之所以引起很多人的关注，是因为汇款领域长期以来一直被认为可能会被区块链上的点对点支付所打破。然而到目前为止，比特币能够让汇款成本降低这个说法遭到行业内许多人的反对，例如MoneyGram（速汇金业务）和西联汇款，都试图描绘现金作为支付手段是不可能被任何数字货币所替代的。项目负责人指出那些被MoneyGram和西联汇款所描述的对于汇款行业的挑战，是因为他们作为行业服务提供商固守自己的想法，缺乏创造性思维。比特币也许是一种解决“最后一公里”问题的创造性解决方案，因为业内认为汇款的主要成本来自运输物理钱币到专门的兑换点。

如果“概念证明”被证明是成功的，也许会通过特定市场与特定的金

融服务伙伴来进入“孵化期”。比特币在这里最大的机会就是可以分割这一切，通过使用一种开发和非专有的标准，可以让本地玩家整合到系统中，从而为你提供一个更加广泛的网络效应。

不同于投资上下通道的方式，像Visa这么大的支付机构可以很简单地利用开放的比特币区块链技术，从而扩展到其网络覆盖范围。其他类似的项目，因为一些相似的结论和理由来支持使用更加私人化的比特币区块链，Visa欧洲和Epiphyte已经创建了相似的内部账本系统，这是通过一个来自Ripple的协议可以合并银行自有账本和分布式总账的系统。

Visa已经有了全球最为强大的支付网络，通过极强的功能性证据，有能力扩展其功能到任何其他支付网络。从这个角度来看，“概念证明”将被视为跨境结算引擎，支持在分布式总账上“实时结算”，并且最终将横跨“多个专有支付系统”。基于比特币的安全性和网络效应，对于像Visa欧洲这样的企业客户，区块链是一个扩展他们的支付系统的理想方式。例如，如果一个比特币供应商倒下，鉴于比特币网络的开放性，将会让用户通过其他提供商来使用另一条支付路径。可以在每个交易的基础上动态传输价格，正因为比特币是一个开放的网络。这并不是说不绑定一个特定的供应商，只不过，你不需要预先知道是在使用哪一个供应商。

Visa欧洲同时也在研究物联网和零售环境中全新的技术，他们认为区块链是一个“非常需要关注的重点”。在Visa欧洲联合实验室中有一小群人正在探索数字货币和区块链，这对Visa欧洲和支付生态来说将会是一个机会。对于Visa欧洲最关键的是，区块链能否让传输变得更快，并且获得更多的扩展能力。

（三）SWIFT

1.区块链路线图

SWIFT，是一个国际银行间非营利性的国际合作组织，总部设在比利时布鲁塞尔，同时在荷兰阿姆斯特丹和美国纽约分别设立交换中心（Swifting Center），并为各参加国开设集线中心（National Concentration），为国际金融业务提供快捷、准确、优良的服务。SWIFT运营着世界级的金融电文网络，银行和其他金融机构通过它与同业交换电文（Message）来完成金融交易。除此之外，SWIFT还向金融机构销售软件和服务，其中大部分的用户都在使用SWIFT网络。

但SWIFT显然已经被这些新兴崛起的金融科技所威胁，一些区块链初创企业和合作机构开始提出一些全新的结算标准，例如R3区块链联盟已经在制定可交互结算的标准。一旦形成全球性的标准，SWIFT很有可能被边缘化。

因此，在2015年12月，SWIFT宣布将于2016年初开始实施新计划，通过使用更快更安全的跨国支付手段——通过整合类似于区块链这样的全新技术来提出一个全新的路线图，以提升其跨行支付结算的竞技能力，并将银行业务在速度方面达到“像光速一样快”。它的市场部全球负责人雷莫克斯（Wim Raymaekers）表示将会改变一下跨银行结算，也许会使用区块链技术来替代双边通汇的对应账户。这样在两个跨国账户之间nostro/vostro（国外/我方）结算的改变涉及消息层和结算层。

雷莫克斯解释说，“随着时间的推移，你必须要在需要的时候进行提升。这就是一个战略路线图，但是你没办法简单地直接去掉过去的系统然后换上新的，这显然不现实。银行已经在它们的系统中内置了这套合规性，你必须要保持在这个层级的控制。”SWIFT表示将继续开发全新的和更好的服务，利用SWIFT的Innotribe机构来进一步拓展互联网金融社区，探索能够实施付款跟踪的支付系统，使用点对点信息传输和区块链技术。

2.构建分布式总账平台

由于区块链技术有可能会取代金融中介机构，这个问题已经被区块链行业创新者和互联网金融专家问过很多次了。SWIFT可以视为是“全球金融行业的主心骨”。那么，SWIFT会如何回应这个潜在威胁的问题呢？

该金融信息型服务供应商在2016年4月宣布，他们正努力构建自己的分布式总账平台。目前关于SWIFT开发此技术的具体细节尚不清楚，但是SWIFT确实表示其概念证明机制目前正在探索如何把分布式总账融合进SWIFTnet PKI保护层，同时用现存的电子数据标准来评估其可操作性。

至今，SWIFT还不相信分布式总账能够“完全满足金融社区的要求”，甚至其服务的11000家金融机构也有同样的疑问。使用分布式总账进行消息传送的机构已经有了一些进步，通过科技支付服务的供应商，包括CGI集团、Earthport和IntellectEU，都在提供基于Ripple技术的产品。

有一些合伙人认为这是让他们能够进步的好事，然而更多的先进分子如巴克莱银行的西蒙·泰勒（Simon Taylor）称其为“迟了两年的赞同”。Needham & Company的股票研究助理斯宾塞·鲍嘉（Spencer Bogart）很好地总结了全部的观点，他把这称为区块链市场主导的迹象。鲍嘉说，SWIFT的声明是多余的，区块链行业人士早就知道，区块链技术会对金融中介机构造成威胁。

当泰勒在其声明中做出激烈的辩驳时，大多数受访者表示SWIFT的计划可以被解读为该公司已经在金融市场受到了威胁。西北航道首席执行官亚历克斯·泰普史考特（Alex Tapscott）争论到，说区块链技术会取代SWIFT还“过于笼统”了。他建议，SWIFT的战略核心应该是用区块链技术彻底改造自己。

康·泰普史考特（Don Tapscott）（**Blockchain Revolution**一书作者，中文版《区块链革命》将由中信出版社出版）认为应该把这次区块链改革看作是积极的，他说，金融行业一直都乐于接受新技术，思维模式陈旧的领导者是最难接受新技术的。

至今还有人报告持有一种非常挑剔的态度，他们觉得该技术还是没有提供充足的市场细节。各种各样的受访者包括：电子交易咨询公司Consult Hyperion的创新主管戴维·博驰（Dave Birch），公共政策研究组织Cato Institute（卡托研究所）高级研究员吉姆·哈珀（Jim Harper），他们都表示对报告中的语言和想法感到困惑。

博驰认为该报告讨论了SWIFT创新实验室的一些概念证明机制，但是没有提供足够的细节证明其合理性。他尤其引用了一些分布式总账的正面影响，包括“交易可追踪性”和“传播信息的高效率”，他认为这些技术目前还是比较薄弱的。

总体上来说，哈珀对报告的评价也并不乐观，不能因为一些区块链网络的推断，就想解散SWIFT。他认为在SWIFT系统下，分布式总账发展的机会很小。斯宾塞表示，SWIFT面临的巨大问题是其分布式总账平台应该如何发展，在其他机构掌权的情况下如何实现中心化。

目前仍然与SWIFT合作的产品及服务的受访者，仍然对声明持有一种积极的态度。IntellectEU业务开发副主席汉娜·祖布科（Hanna Zubko）表示中介商解决方案公司“经常建议”SWIFT应该接受分布式总账。祖布科称赞了SWIFT是一个可靠的创新伙伴，同时该公司也接受分布式总账生态系统。她认为没有什么事情经过一夜就可以完全改变，至少要谨慎地采取第一步措施，同时朝着正确的方向发展。同样地，在CGI集团负责区块链开发的迈克尔·劳克林（Michael O’Laughlin）说，他把这次声明看作是批准公司使用分布式总账技术的信号。

博驰推断即使分布式总账技术被广泛接受，还是需要一个像SWIFT

这样的机构，他确信分布式总账的实现会取代SWIFT系统——可以想象银行会有SWIFT通道，但SWIFT不会作为中间商因为每个通道都有账本——但是不会取代SWIFT机构。

（四）微软

1.Azure

2015年10月，以太坊项目和ConsenSys，这两个项目的共同创始人之一，宣布已经和全世界最大的企业软件供应商之一的微软建立了合作关系。将会在微软的Azure云平台上，为其企业客户提供开发工具。旗舰产品将会包括BlockAppsStrato——一个能够构建以太坊应用的工具包，和Ether.Camp——一个区块链浏览器。

美国微软金融服务部的技术战略总监马利·加里（Marley Gary）表示，他们已经看到许多有潜力的框架专注于金融服务，而像以太坊这样的跨金融机构的平台，能够把许多还停留在过去的人拉到现代。对于开发基于分布式总账的应用，他们认为以太坊的确是一个非常好的平台。

通过在微软的Azure云平台上，开发人员可以创建半私人的或者纯私人的网络环境，而不用花费任何资金。

在某些时候你可以打开一个公开节点，在集成开发环境中，通过点击按钮就能把你的调试程序部署到公开的以太坊区块链上。这将花费价值2分到5分的以太币，这样你的应用程序就可以部署了。人们大约会花费1分钱或者不到1分钱来使用你的应用进行互动。

潜在的应用将会包括由银行组建的联盟之间进行期货汇款交易或者搭建公开交易所。微软将会和ConsenSys一起协作，但是微软并没有购买以太币，加里表示说，微软仅仅是为客户提供一个可以使用

ConsenSys的平台。

作为项目的一部分，卢宾（Lubin）介绍说他们已经在这个系统中开发了一系列的应用程序。公司表示他们涉足的应用范围相当广泛，无论是有趣的还是严肃的项目都有。如DAOWars（人类玩家可以设计一个自动代理机器人来对抗其他竞争者设计的机器人），又如GroupFnosis（预测市场平台）和EtherSign（应用于文档管理和签名的加密工具）。

微软和ConsenSys之间合作的第一个成果在2015年伦敦召开的以太坊开发者大会上被宣布。

2.BaaS

微软公司不仅在区块链技术上看到巨大的潜力，同时也认为其中蕴含巨大的商机。在微软Azure云平台上，将会通过部署包括以太坊在内的区块链基础设施，为客户提供“区块链即服务”（Blockchain as a Service, BaaS）。

据微软Azure的美国金融服务技术战略部门主任马利·加里说，区块链和其所在的整个系统发展迅猛。无论是“云”端还是本地，或者是混合的分布式总账的开发、测试和部署领域，微软的Azure都将会做到最好。

基于区块链技术带来的优势，一大批有兴趣的企业（尤其是金融服务业）开始接受它并从中受益。这是微软正在挖掘的机会——它希望银行和金融公司使用Azure云平台来承载其区块链。

加里表示，在区块链行业，他看到了巨大的商机。在未来的几年中，企业级的区块链基础建设作为编织这一金融基础设施的基础，将会非常重要。

事实上，微软在区块链的项目上已经与许多初创企业和大公司有合作。在微软Azure的BaaS系统中，现有的合作伙伴包括ConsenSys、Ripple、Eris Industries、CoinPrism、Factom、BitPay、Manifold Technology、LibraTax和Emercoin。

微软Azure BaaS的最新进展是MultiChain和Netki的加入。Multi使组织能够快速设计、部署和操作分布式台账；Netki设计解决方案，使基于区块链的产品的操作更加便捷。

此外，Azure的BaaS还宣布了新的开发/测试实验室的整合。报告中指出，目前使用的Azure的开发/测试实验室将会使区块链技术变得更加易于构建和测试。现在所有区块链相关的服务和合作伙伴可以在实验室环境下作为物品来设置和添加。

区块链的分布式总账是以“有权限的”或“无权限的”方式，防止记录和存储的数据被篡改。已有多份报告阐述分布式总账技术的优点和成本优势，吸引实体经济进行实验。世界经济论坛调查报告预测，到2025年，全球GDP（国内生产总值）的10%将用区块链技术保存。

大多数版本的区块链还处于起步阶段，在这一技术正式投入生产之前，测试和提炼的过程将会持续下去。微软表示，这不仅为各种实验项目提供了平台，为这一过程提供了保障，而且已经准备好把Azure的BaaS平台变成一个重要的营利来源。

3.帮助大银行开发区块链技术

2016年4月，微软宣布已与由多家大银行组成的区块链联盟R3 Consortium达成合作协议，将帮助开发区块链技术。

微软和由摩根大通、花旗银行等国际大行组成的R3 Consortium联盟表示，它们将会携手合作，“加速这种被称为区块链的分布式总账技术

的普及”。

根据双方达成的“战略合作”协议，微软Azure将会是R3的云服务提供商。双方称，微软将会为R3提供基于云端的工具、服务和基础设施，以及技术架构师、项目经理、实验室助理和支持服务。

微软全球业务拓展执行副总裁佩吉·约翰逊（Peggy Johnson）表示，有了智能的云端技术，R3及其银行成员将能够加快实验和学习进程，并加速分布式总账技术的部署。R3及其成员还将能够接触到微软的区块链合作伙伴，其中包括Ethereum和Ripple等创业公司。

（五）IBM

1.区块链战略

2016年2月17日，IBM公布了其全面的区块链战略，这让IBM的“区块链战略大戏”终于达到了高潮。IT巨头IBM第一次对基于区块链新兴技术的商业解决方案展开深入的研究。

尽管之前IBM就已经主导了Linux的超级账本项目，并将自己的论文向其他技术提供者开放，但本次宣布的消息可以说是全面发动攻击，标志着IBM已经全速进军区块链行业，其研究的深度和广度在同行业中都是独一无二的。

IBM透露战略的中心内容是，多年的战略规划，包括BaaS与公司既有的资产整合，例如IBM z系统，该系统是全球前100名银行的核心IT系统；Watson物联网（IoT）平台，以及它的开发工作组项目Bluemix Garage。IBM已经成为第二家推出BaaS服务的科技巨头，另一家是微软，微软在2015年10月公布了其沙盒开发计划，在区块链行业中掀起了一股热潮。

IBM区块链技术副总裁杰瑞·柯摩（Jerry Cuomo）详述了公司市场战略的特别之处，他认为，用户使用IBM的区块链项目服务后，可以迅速测试区块链网络，这些特点是对微软进行补充，但是强调他所认为的最大的潜在差异。柯摩认为微软在既有的区块链网络上更为开放，然而对于IBM的BaaS服务，商务客户将会使用IBM区块链结构，因为这是IBM精心制作的一种受专利保护的公共服务。

柯摩认为IBM的最新共识算法改进了隐私保护和可审性，商务客户可以为更广的用例创建区块链应用，而创建速度无可匹敌。

平台的最初用户包括一些知名企业机构，例如伦敦股票交易所（LSE）、Kouvola创新和日本交易所，东京股票交易的操作员认为由于上述大型机构的加入，也让很多企业用户产生了共鸣。

2.区块链的DNA

IBM表示，他们设计的区块链结构与其他既有区块链网络有些不同。

他们所指的区块链“结构”是指“区块链的DNA”以及一种商业网络，在这个商业网络中，交易可以被复制，用户成员可以访问共享账本。

这里的账本有三个特性，第一，可复制，当你输入数据时，该数据会复制到所有的账本中，即所有的账本都是同步的。第二，它拥有特殊权限，你只能在你的权限范围之内浏览有限的账本，也只能在这些账本上进行商业操作。第三，借助这种区块链结构，用户可以创建含有逻辑性的交易，例如可编程的合约，该合约可在特定时间段内，处于特定条件下自动管理一笔资产。这种结构使分布式总账成为可能，加快网络创立的进程。

IBM指出，开展这项服务可以在“可插结构”中起主要作用，用户将

体验多种软件模型，加密身份管理工具可在Java和Golang中写入智能合约。此外，通过隐私和机密控制操作，用户可以设置权限，明确谁可以浏览账本，谁可以执行智能合约。

这项功能与当前的公共区块链大为不同，例如比特币和以太坊，在比特币和以太坊中，所有人都可以加入到网络中参与操作。而IBM的智能合约用大众更熟悉的开发语言写出，而以太坊却全部用新语言写出。

3.与超级账本互动

BaaS服务的一些特性与超级账本项目相重合。超级账本是另一个合作项目，截至目前共汇集了30多家行业利益相关者，包括初创公司，传统金融机构和潜在的终端技术用户，各方的目标一致，即创建一个开源区块链服务。

IBM的共识算法将会使用IBM贡献给超级账本项目的4.4万行代码，但由于附加价值的服务，这种共识算法还是有所不同。这种共识算法所使用的都是基于那些编码，而不是编码之上的价值；所增加的是精心创立的区块链网络能力，以及一系列样本和服务。

作为一个测试环境的例子，IBM将一个区块链应用样本上传到其网站之上，开发者可以在此应用上测试资产交易。

IBM尝试在其网站上提供更多的内容，网站中有一个还未开放的界面，其中包括“智能合约研究者”，开发者可以利用这个界面，体验智能合约，还有一个“汽车租赁”界面，为大家提供一个基于区块链的供应链端应用全景。

4.对合作持开放态度

IBM将BaaS服务描述为一种能够让用户在云端协作的技术，用户可

以通过这种技术与其他同业者进行交流。如同Azure服务，这项技术还处于测试阶段，首先对开发者开放，之后达到规模化的目的，最后公开发布区块链的生产版本。

日本交易所也有这个目标，日本公司研究的“概念证明”，旨在创新低流动性资产交易系统。他们在使用IBM的测试服务，目的是进行分级。根据日经指数（Nikkei），日本交易所想发表一份报告，主要是关于2016年末他们对工作研究的最新发现，而伦敦股票交易所（LSE）指出他们在创立一些风险管理的项目，并提高全球市场的透明度。

IBM承认超级账本项目和他们的工作之间有交集，而且日本交易所也加入了超级账本技术研发，事实上，正是应日本交易所的要求，监管者才加入该项目。

IBM表示，加入的交易所希望其监管者也能访问编码，所以监管者也参加了超级账本项目。但是IBM与监管者的工作关系是托管式服务。IBM的共识算法相关的商业业务和超级账本项目向监管者发出了积极的信号，即监管对象希望他们的项目符合全球政府机构的要求。这也是加入开放式环境的另外一个原因，监管者不想对所有的区块链结构做背书，但是IBM希望通过这种措施，也许他们会背书一两个结构。

5.迅速面向市场

IBM服务的关键在于，它可以撬动既有服务系统，例如IBM z系统，这是IBM的大型计算机和分布式服务器技术系统。在IBM的网站上，IBM宣传说它的z系统可以将区块链带入“一个新的高度”，因为该系统可以处理“大规模的交易数据”。通过接口交易记录系统以及访问z系统上的既有数据，可以加速估值时间，降低成本，简化程序。

通过z系统，用户可以“调整他们自己的结构”，在网络中传递信息，寻求同业人员认证时，对交易进行加密。z系统由于其出众的大规

模加密性能而被大众所知，所以如果在z系统中运行区块链系统，那么其规模化将轻而易举。z系统就像是专门为这种工作量而准备的。

IBM也将推出IBM区块链DevOps服务，客户可以在12秒内创建微型区块链网络。同时，为了让潜在客户更好地理解其技术的这些层面，IBM正在伦敦、纽约、新加坡和东京启动IBM Bluemix Garages，目的是寻找区块链概念证明的设计和实施的开发者提供个人支持。

IBM还将为客户提供和相关专家一起参加“90分钟互动会议”的机会，这些专家能够帮助他们快速实施自己的想法。远程呈现和网络会议同样也对客户开放。IBM相信客户会发现这其中的价值，他们能够利用团队的知识让技术以最快的速度得到应用。

（六）Infosys

2016年4月，在Infosys Confluence旧金山会议上，IT服务巨头Infosys最近通过其分公司EdgeVerve Systems发布区块链平台。

Infosys是印度历史上第一家在美国上市的公司（纳斯达克股票代码：INFY），总部位于印度信息技术中心——班加罗尔市，在全球拥有雇员超过100000名，分布于27个国家的56个主要城市。Infosys公司的主要业务是向全球客户提供咨询与软件等IT服务，经营理念是采用低风险的且在时间和成本等方面可预测性高的全球交货模式（GDM），加速公司的发展。

该项目被称为EdgeVerve区块链框架（EdgeVerve Blockchain Framework），致力于深化金融服务业的区块链技术应用。Infosys表示，该平台建立在许可型分布式总账的基础上，可以使银行“快速部署”区块链服务。

EdgeVerve在宣传材料中描述分布式总账平台为不受资本类型限制的、高度扩展性和“最小化金融服务运行和交易成本”的最佳选择。该平台专门为银行业设计开发，可以扩展到国际跨境交易所需要的水平。这些技术优势使该框架内的应用平台能够运行支付和高容量地交易这些银行业务。

EdgeVerve客户和业务总裁安迪·戴伊（Andy Dey）说，公司将投资爱尔兰的相关项目研究所，并与几个未具名的机构合作探索其应用。EdgeVerve表示，已经围绕数字数据库、发票处理、支付、智能合约、银团贷款和贸易金融展开概念证明研发工作。

就在数周前，Infosys曾公布相关技术理论研究，公司相关领导表示相信未来几年内区块链技术会渗透到金融业，尽管同时存在相反的观点。Infosys通过该平台，加入微软、IBM和红帽（Red Hat）等IT巨头的技术探索大军，在企业区块链解决方案的新兴市场中争夺业务。

三、咨询巨头的区块链案例分析

（一）德勤

德勤会计师事务所（Deloitte & Touche）是世界四大会计事务所之一，为德勤全球（Deloitte Touche Tohmatsu）在美国的分支机构，后者在126个国家内共有约59000名员工。

1.德勤数字货币社区

继花旗、瑞银、USAA等银行巨头之后，全球四大会计事务所之一的德勤，成为目前对区块链技术感兴趣的最新主流金融机构。该公司透露其正在尝试将区块链技术应用到客户端的自动审核及众包（公司以自由形式外包给非特定大众网络）公司在应用程序上的咨询服务。

德勤公司首席咨询官艾瑞克·皮斯尼（Eric Piscini）表示，德勤一直在对区块链技术潜在的商机进行研究。公司有20万雇员，所以他们需要对区块链及其底层技术有更多的了解，并且相信它真的可以改变客户的经营方式以及他们的运作过程。公司将这个团体命名为“德勤数字货币社区”（Deloitte Cryptocurrency Community, DCC），该团队在全球12个国家中有约100名成员。目前主要将精力集中在告知银行业及零售客户区块链技术的优势，同时起到协调实体店与产业初创公司间关系的功能。

DCC社区有三个任务：

（1）培训德勤及其客户群抓住机会；

(2) 研究该技术如何提升现有服务水平；

(3) 所说的比特币使用案例有如下几个：货币交换协议、管理员工薪资支付、央行拥有的数字货币的可行性。

2.两大阵营

德勤表示，他们的许多客户目前仍处于对区块链技术的探索阶段。大多数公司还在尝试区分比特币和其他区块链间的差异。然而，还有些客户正在将这一技术应用到具体某个方面，比如增加额外收入或降低成本。德勤透露，有一小部分的客户已成功将区块链技术应用到具体业务实例中了。因为通常当某一新技术发展到第三阶段时，他们才会开始分析这一技术并且好奇如何将其应用到具体业务中去。这些客户正在寻求建立在比特币之上的其他协议，包括Blockstream协议（核心为侧链技术）、合约币协议及Factom协议（核心为应用程序开发）。关键问题是，现有协议究竟是在与这些公司合作还是在创建一个私人区块链。

瑞波实验公司和以太坊研究的区块链替代产品目前也处于探索阶段。对于德勤来说，两边都有其客户。他们想使用Factom协议，因为这是个很好的解决方案。于是他们将一个抽象概念摆在了德勤和区块链之间。一种看法是，不必非得让他们知道我在用比特币，但是我的确在支持他们的业务、大型社区和大型挖矿网络时加入了这一技术。另一种看法是，有些人说我不想和比特币扯上任何关系。因为我不想和比特币打交道，我打算用以太坊。这就是所谓的两大阵营。

皮斯尼认为德勤在纽约的银行客户，主要对使用区块链进行交易、转账结算等感兴趣，其他地区的零售客户则对区块链能起到像礼品卡提供商Gyft的奖励作用感兴趣。德勤表示，目前就区块链技术在公司业务上尚未确定某个具体的计划，而这恰好说明公司想把区块链用在最合适的地方。目前的想法是，找到最适合用这一技术的地方，来创造更多收入、产生不同的客户体验或者降低成本，找到之后再植入技术来实现这

些目标。

也许最值得关注的是德勤作为初创企业和企业之间的调解人作用，目前这两个团体之间的交流尚不平稳。一些相对传统的公司仍找那些不会把技术和业务衔接起来的“科技极客”寻求帮助。现实的确如此，很多初创公司缺乏经验，也不知道该怎么和客户谈生意，事实证明，如果你没有用对正确的术语，对方连10分钟的时间都不会给你。截至目前，这已经让大公司对该技术产生了“错误的预想”。比如，德勤注意到，还不能证明区块链可以高效低廉地取代共享型数据库。一些大公司已经假定了区块链可以解决商业或技术上的问题，因此他们对其抱以极高的期望。有些时候，德勤会告诉他们，区块链只能帮到这里了，贵公司应该考虑其他的解决方法。

区块链正在成为一个流行语，人们试图用它来解决所有出现的问题，尽管有时候人们还弄不清楚区块链究竟是怎样起作用的。专业人士正在想让该技术转行，因为这样他们才能想出合适的解决方案。但相互理解可能需要几年的时间。

3.德勤区块链平台Rubix

德勤已推出软件平台Rubix，它允许客户基于区块链的基础设施创建各种应用。Rubix被称为“一站式区块链软件平台”。Rubix官网罗列了该软件的四个利益方面，包括贸易合作伙伴关系、实时审计功能、土地登记功能以及信用积分。公司内部则专注于通过隐秘方法自动解决审计处理中存在的问题。

因为公司的每笔交易都在区块链上进行，所以利用区块链设计出的解决方案将会加快审计进度。同时由于区块链具有不可逆性和时间戳功能，对于需要审核的公司，德勤会核查该公司的区块链及全部交易。这将加快审计进程，使其更便宜、更透明。

Rubix发布于R&D之后大约一年，德勤目前已经具有了这种平台，可以帮助德勤的商务客户。客户才刚刚认识到，未来建立在区块链技术上的无限可能。大部分的客户以其行业、目标和需要来确定以及执行计划。德勤将他们对技术的理解，与技术对客户生意所产生的影响相结合，不仅仅是今天他们继承的商业遗产，而且对未来两到三年客户生意的一个预测。

在服务中推动各方兴趣的关键在于：金融服务提供者想急切地确定区块链技术如何成熟，然后他们就可以开发出一套有远见的商务战略。Rubix的团队目前正在与一家医药健康领域的客户合作，准备建立一个方便支付的模型。Rubix透露，客户的需求是这些“概念证明”，将会向组织中剩下的人提供提醒或给出信号，告知他们各自的组织，未来会发生什么……其他可能的关注区域，将会研究应用的信用积分和供应链系统，在这两个领域，自动化将会改变现有的商务操作。某些过程的自动化将会产生重大的影响，可以提高透明度和开放账本，如果你能在既有的过程中提供效率，那么这些就是技术的非常有价值的贡献。

也许Rubix最令人瞩目的特点，是它为客户提供多种分布共识平台。截至目前，Rubix已经在以太坊协议上集中了大部分的工作，就提供功能性而言，企业客户对此非常感兴趣。

主流金融服务提供者在私有链和许可链上有不少兴趣问题，但是那些主流金融服务提供者也许方法不对，所做的努力可能达不到预期效果。例如，很多大型金融机构对比特币成为数字货币保留意见，而他们继续追求那些人们已经不再使用，或者有限度使用的项目，例如数字代币。但是，奥里斯·瓦利安特（Oris Valiente）指出为了确保分布式总账系统运行，仍然需要代币化。瓦利安特深信未来，数字货币一定会成功，因为数字货币有一个光明的未来，尤其是在新兴市场，国家发起的货币或数字货币，为那些被排除在金融服务之外的人们，提供了更多参与世界经济的机会。

但要让发达市场的主流接受数字货币，还有很多困难需要克服。比如在发达市场，已经有消费者和其他替代产品，数字货币会占据主导地位吗？也许发达市场的人们不缺金融产品工具，只是要看人们如何理解这种技术，后者将成为主要的障碍。就此而言，客户是将区块链技术视为在新兴市场中，创造新产品的一种方式，在这些市场中之前几乎不可能创造或分配新产品。一个最恰当的例子就是保险业，人们可以使用区块链技术，解决投保人与保险人之间信任的问题。如果区块链技术可以作为新兴市场P2P保险平台的一个促进器，那么，就等于为整个社会创造可带来价值的新产品，也就将向实现金融准入和消除贫困前进一步。因此，一旦区块链技术走过探索阶段，进入巩固阶段，这种转变将很有可能发生。就像是一旦你看到这些细小的碎片最后汇集成一个全面的网络，那时你就会感受到很多有意义的影响，而这些影响将在一两年之后发生。

4.德勤不可取代

德勤不认为P2P（区块链技术的核心）技术有可能会取代类似于德勤这样服务供应商。失败的可能性是很有限的，但这个机会是不能错过的。之前的例子将改变德勤今后的工作方式，但并不认为德勤会被（区块链）替代，只是业务处理更有效率了。至于在纳税服务方面，由于技术尚不明朗但有可能获得业务。此外，德勤还看到了技术在咨询服务方面的应用机会。

在咨询方面，德勤将会见证生态系统从适应、改变至将区块链作为解决方案的过程。其潜力在于通过P2P众包平台提供大范围的咨询服务，而不是帮助客户制定发展策略。顾客可以在区块链上进行咨询，然后区块链将针对顾客的问题匹配合适的公司（来解决您的问题）。正是考虑到咨询逐渐成为德勤业务的重要组成部分，公司“非常认真”地对待这一发展过程。

即便是企业用户，目前最受关注的仍是区块链技术能否被广泛应用，但支付功能作为核心功能仍将受到比特币和区块链的影响。站在德勤的角度看，比特币应被当作一种为全部交易（包括金融行业外）提供服务的技术。当你想对各种类型的交易进行管理时，比特币是一种非常有意思的应用。你和我之间可以互传比特币，也可以让司机来接机。今天我用优步打车，但明天我可能用区块链打车。而随着时间的推移，区块链将在资产转让、智能合同、投票表决等事宜上逐渐成为一个基础层，而且有可能针对不同的用途创造出不同的区块链。像比特币这样的数字货币就很有可能继续在区块链的管理中发挥作用。

尽管德勤正在研究的用例超过20个，但他们仍表示并不清楚哪种机会是区块链最好且最直接的用例。德勤预计将会有一款“杀手级”的应用面市，而公司可以从中获得极大的利益。

5.建议央行发行数字货币

2015年7月10日，德勤发布了一份报告，探讨如何让央行发行自己的数字货币。这篇报告题为《国家担保的数字货币：将比特币最佳的创新应用于支付生态系统》，该报告设想了一个与比特币类似的生态系统，其中金融机构扮演无偿的矿工，而整个总账系统由中央银行负责管理。

由央行发行数字货币，这一想法其实很早就被提出，已有的概念如美联储币（Fedcoin）以及由新加坡央行提出的评论。理论上来说，由央行发行的数字货币，央行能够控制货币的供应量，而网络上的数字代币能够与由央行发布的法定货币相联系。

德勤认为，这样的实验是值得追求的，尤其是像美联储这样寻求改善型数字支付方式的机构，该报告指出：好的结果就是，这种新型支付方式将彻底改变现有的系统，其具有降低成本、减少错误、提高资金转移的效率，平衡隐私和匿名性的潜力，并且它无须一个中央式的组织来

每天负责维护，这可能会真正地成为变革。

当然，由德勤假设而出的央行数字货币，与比特币之间存在关键的区别。例如，这种央行数字货币并不对网络的代币数量设限，而比特币的总量上限被设定为2100万。央行将控制其发展，并决定哪些实体验证交易。此外，央行将提供面向用户的服务，例如钱包服务，根据德勤的报告，用户将保留私钥的控制权。

至于央行究竟如何去控制这种系统中的货币供应量，德勤给出的建议是：为了增加货币供给，央行可以实时转账数字美元（crypto-dollars），从它的私钥传输到不同金融机构的私钥里。为了缩小货币供给，央行可以提高准备金要求，而金融机构将加密美元传输到央行的私钥，从某种意义上讲，在功能上它等同于当前的系统。所以，由央行发行的数字货币，可能不会替代比特币或任何其他数字货币及法定货币，这种概念，某一天会使数字货币的生态系统更为广泛。

6. 质疑监管过早

2015年10月21日，德勤公司发表了一篇报告，称当前去尝试监管比特币是否还为时过早。在这篇题为《比特币处在十字路口》的文章中，德勤谈到了比特币和区块链技术的优势，探讨了监管数字货币是否对于它们在未来的发展及大规模的普及，会产生负面的影响。德勤认为，在很多方面，政策制定者和监管者的行为，皆是遵循自己的使命宣言，保护公众和金融市场的诚信，那么一个重要的问题就会随之产生了，现在去尝试监管比特币，是否还为时过早呢？

文章提到了一些历史的证据，试图说明，不对新技术的发展进行干扰，即为最好的行动，并指出了三个原因，解释为什么全球政策制定者，应避免在比特币萌芽期对其进行监管。首先，比特币的市场渗透率，相较于传统的法定货币系统和交易平台而言，还是比较小的。比特币受到了世界各地政策制定者和监管机构大量的注意以及审查，远远超

出了其目前的规模和市场影响力。事实上，从任何相关的指标来看，比特币目前的价值风险，也只是金融业海洋中的一滴水。其次，其他变革性的技术，往往在受到监管之前，会拥有更多的时间来进行发展。作者援引了电话（发明于1876年，于1913年才受到调控）、飞机（发明于1903年，于1938年受到调控）、互联网（发明于1969年，最近才被加强调控），以及比特币这个开源平台（最先是于2009年发布的）来说明。比特币的发展仅仅经历了6年的时间，根据以往的新技术例子来看，它距离实现大规模的普及，还有很长的路要走。最后，比特币目前尚未发现其最具价值的应用，它和区块链技术的潜在应用名每天都在扩大，当前还只是处于早期阶段，但其中一些新出现的应用，已经让人非常兴奋了。

7.与Colu进行合作

区块链初创公司Colu透露已经与跨国咨询公司德勤达成合作协议。它在2015年8月推出了区块链公测项目，并表示这次合作将为区块链技术带来全新的“大市场”。尽管该公司没有公布此次合作的细节，但是该项目将涉及Rubix软件平台，德勤客户可在该平台上建立自己的应用程序，包括在区块链上建立票务系统和登记系统。

Colu公司的首席执行官阿摩司·梅瑞认为，过去的两个月里，他们一直在与德勤代表沟通，并与德勤在加拿大的分公司以及Rubix开发团队建立了密切的联系。因为德勤已经尝试为一些客户提供不同的有趣用例，所以德勤需要Colu在技术方面以及在定义不同的“概念证明”上提供帮助。

在2015年7月时，有四大会计师事务所专业服务机构透露，它们已经发现了超过20种区块链技术的用例，并且已经对这一领域的研究超过18个月。在短短的三个月时间里，Colu就已经与超过20家公司建立了合作关系，包括音乐平台Revelator、加勒比比特币交易所Bitt，现在又增

加了德勤。对Colu而言，看这些不同的公司如何使用区块链技术建立不同的应用是一件非常有意思的事情。他们正在追踪这些不同的用例，并且希望未来能够开发出更多有趣的应用。

8.黑客马拉松

万向区块链实验室和德勤于2016年1月，在中国上海举办了全球区块链黑客马拉松接力赛。参与者分成若干个小组，在两天时间内“头脑风暴”碰撞出区块链的创新应用，并完成演示版本的设计与开发工作。以太坊开发团队、德勤Rubix团队、万向区块链实验室技术团队等区块链技术专家在比赛期间全程为参加者提供技术指导。在完成开发后，每个小组向大家展示了该小组开发的原型版本，并瓜分了由组委会提供的高达10万美元的丰厚奖金。

在2015年成立的万向区块链实验室（WanXiang Blockchain Labs）是一家专注于区块链技术的非营利性前沿研究机构。实验室聚集了领域内的专家就技术研发、商业应用、产业战略等方面进行研究探讨，为创业者提供指引，为行业发展和政策制定提供参考，促进区块链技术服务于社会经济的进步发展。

9.5个合作伙伴和20个用例

2016年5月，德勤表示已经同包括BlockCypher、Bloq、ConsenSys Enterprise、Loyyal以及Stellar在内的区块链初创公司建立合作关系，并且开发了一系列业务模型，包括保险、员工管理以及跨国支付，包括20个技术原型。

在银行领域，两家初创公司帮助德勤在区块链上建立了所谓的“数字银行”。虽然这种银行并不是在区块链基础上从头建起的，但是其构造的不同业务组件目前已经出售给了银行。加利福尼亚的BlockCypher是德勤的新合作方之一，这家公司目前已经筹得350万美元的风投资

本，为德勤提供了核心技术，即一个应用程序界面层，来运行以太坊、比特币区块链上各种数字银行工具。此外，还提供了各种定制的私链。

德勤表示，这些合作方代表的是各种各样的业务种类，而德勤则致力于在全球建立战略合作，从而推动区块链技术从理论发展到现实世界的应用。纽约的ConsenSys Enterprise是德勤早期区块链合作伙伴，它正在帮助德勤建立一系列出售给银行的金融产品原型。这家公司是ConsenSys众公司名下的一家，正在建立各种以太坊区块链的公共及私人产品。德勤把BlockCypher、ConsenSys以及Bloq归为一类，这反映出对这三家公司帮助德勤扩大区块链全球应用的厚望。但是，德勤又指出Bloq与其他两家不同，它不是银行业，这家芝加哥公司的任务是为德勤开发非区块链技术保险产品。

初创公司Loyyal，前身是Ribbit.me，就专门研究奖励机制；另一家Stellar则致力于跨国支付。Loyyal在它以Ribbit.me的名义建立区块链驱动的奖励平台时，就筹得了150万美元风投资本，德勤认为这一原型能够改变各行各业员工的行为。而Stellar则与其他合作方不同，它是一家非营利基金会，目的是推动跨国支付的发展。Stellar同德勤的合作项目是为北美之外的银行专门建立金融领域的服务。

这五家合作者中，有三家已经获得收益，德勤并没有透露是哪几家，也并没有去预估每家公司能够带来的潜在收入。相反，它消除了任何阻止区块链在各领域及相关部门应用的障碍，从而挖掘各行各业的潜在需求。这样，公司扭转了传统工程关系，以专心满足这些需求。

如今除了银行业，其他领域的扩张也愈演愈烈。在保险、医疗保健、零售、销售，或者笼统地说——商业领域，其实都存在很多机遇。德勤的客户已经要求区块链产品覆盖更多领域了，比如保险、石油及燃气、资产管理等。德勤透露，它有一个“大型的使用案例库”，相信跨国支付意味着能够有值200亿美元的突破性机遇。

（二）普华永道

普华永道（Price waterhouse Coopers, PwC）是一家全球集团，有超过20万名的雇员，主要集中在美国、欧洲和亚洲，在2015年有350亿美元的收入。它被认为是世界四大会计事务所之一，也是美国第六大私人企业，财富500强中有35%的企业是由它进行审计的。在2015年，它吸引了财富100强中43%的审计费用。而现在，它把目光投向了区块链。

1.对2016年的三个预测

杰里米·德雷恩（Jeremy Drane）是普华永道中，致力于研究美国互联网金融，区块链和智能合约的高级主管，凯瑟琳·马什（Cathryn Marsh）是普华永道FSI研究所的主管，该研究所致力于新技术情报对于金融服务业的研究和分析。他们二人在2015年底发布了一篇对2016年区块链行业发展的三个预测，勾勒出未来一年中区块链技术的发展趋势，以及这些发展趋势中的关键点。

在PwC看来，区块链技术极可能导致在金融服务行业内出现完全不同的竞争力，现有的盈利方式将会被彻底颠覆，那些拥有全新高效区块链平台的拥有者将成为最终的赢家。

预计在新的一年时间里将会出现很大的变化，并且其中有三个大的趋势将会是非常重要的：

（1）传统金融机构将会在探索他们与客户、供应商和竞争者新的合作机会时，寻求需求保护他们的知识产权；

（2）大型金融机构需要在设定战略规划时确立自己的风险控制参数；

(3) 市场参与者将会围绕着交易层面来开发相关流程。

那些传统的金融机构，如银行和交易所，正在寻找各种方式来改进和提升各种类型的交易，而那些非常了解这种全新技术的初创公司和服务提供商们也正在努力更好地接入和部署这种商业模式。当进入2016年，会鼓励这些金融机构进行互相对话合作，了解和分享它们之间的知识产权。

在2015年，大部分市场工作的重点都放在基于交易解决方案的概念证明上。随着金融机构在2016年的大举进入，可以观察到从目前交易事务层面转移到支持系统和流程。该行业需要开始探索治理、审计和IT安全。

也可以看出，金融机构的问题将从“我该如何使用区块链技术”变成“我们该如何充分利用区块链技术建立配套流程”，甚至是“这些全新的流程将会对我们的风险控制有何种影响。”

建议各个企业应该尽早地开始尝试使用区块链技术来测试各种公司内部职能（如合规性、风险和内部审计），这样就不会止步于概念证明，而且更加容易确定资金的投放方向。

新技术带来的好处，往往并不会让市场中每个参与者都受益。换个说法就是，总会有赢家和输家。这种情况下，对于大多数参与者很难将这些技术优势变成实实在在的收益。很可能会看到这样一个未来，精明的市场参与者联合一些少数技术企业（这种战略关系可以称为“微联盟”）将能够把他们成本高昂的内部流程改造为高效和共享的平台。由此产生的平台，将会作为一种服务出售给更小的竞争者。

只有少数几个关键合作伙伴有能力同时协调战略和商业之间的关系，用普华永道的观点来看，这在未来几年将会成核心竞争优势。由于区块链技术的发展速度惊人，可能会让你感觉刚从幼儿园毕业就被送到

了大学。而2016年就像这个幼儿园毕业的暑假，必须在很短的时间里完成大量的准备工作以应付后面的大学课程。

如果要问建议，那就是确保你的学习能力可以跟上你要学习的内容。你会需要一个战略规划，以确定你的重点方向。此外，你还需要对这个技术进行深入的学习研究，以确保你真的可以从中受益。

2.正式进军区块链

2016年1月，PwC正式宣布进军区块链技术行业。他们已经开始组建其区块链技术团队。该团队设立在英国的贝尔法斯特，预计到2016年年底，该团队将会从目前核心的15人扩展到40多人。这些小组将会调查PwC客户对于区块链技术的潜在应用，以及推动金融行业对于该技术的理解程度。

PwC合伙人和EMEA（欧洲、中东和非洲地区）金融科技负责人史蒂夫·戴维斯（Steve Davies）表示，有明确的证据表明，无论是银行、机构还是政府，都在寻找将区块链技术作为一种安全存储和分布式解决方案——当区块链的巨大潜力正在逐渐显现时，PwC将会很好地为其客户提供世界级的相关服务。

PwC英国执行委员会成员阿什利·安维（Ashley Unwin）表示，区块链技术正在让金融服务业中的一些主要参与者感到担心，因为他们不知道它会如何发展，它对于变革目前的商业模式究竟会有多大的潜力..... PwC确信，这个颠覆性的金融科技将会使得整个金融业对于区块链专业知识的需求大幅增加，而他们将会试图成为探索这些颠覆性新技术的领导者。

这已经不是PwC第一次对区块链技术的潜力表现出兴趣。在2015年，该公司发表过一篇题为《货币不是对象：了解不断变化的数字货币市场》的报告，主要探讨如何去理解数字货币，特别是比特币，将会影

响金融行业未来的发展。从这份报告中，就足以看到PwC对于数字货币潜力的认识程度。

3.与Blockstream建立合作关系

Blockstream在2016年1月底宣布，和PwC建立战略合作伙伴关系，为全球企业提供区块链技术和服

Blockstream是由比特币生态圈内一些重要的贡献者成立的，目前正在通过一种称为“侧链”的机制来扩展比特币协议的能力。随着侧链的开发，该企业开始寻求将比特币的区块链技术应用到更多的资产类型，包括数字货币、开放资产和智能合约。

Blockstream的商务高级副总裁亚历克斯·弗勒（Alex Fowler），阐述了这次Blockstream与PwC合作伙伴关系之间的契合点：Blockstream为企业提供了非常成熟的且经过完善测试的安全区块链产品——通过可以交互操作的侧链技术来扩展比特币企业用以支持新的应用——因为他们是整个行业中经验最为丰富的团队。PwC带来了深厚的行业经验、广泛的业务服务和最前沿的客户见解。将其合并在一起，PwC和Blockstream将会帮助企业评估数字货币、区块链技术，以及为比特币协议带来新的用户。

PwC合作伙伴以及Fintech联合负责人哈斯克尔·加芬克尔（Haskell S.Garfinkel）表示，对于PwC的客户而言，了解比特币和区块链上技术新的全球应用，接受它的无数种用途，使用它来提升金融安全性、效率和合规性是非常重要的。PwC正在联合Blockstream来为他们的客户提供两个团队的共同知识和能力——让他们有目标，让两支团队能够最大化地利用专业程度、人才和资产。

总之，和Blockstream的合作将会通过对现有解决方案来帮助他们客户，以及开发新的产品使公司能够跟上新的步伐，采用这种市场颠覆性

力量，并且领导创新。

PwC首席Fintech联合负责人迪恩·尼克劳斯凯奇（Dean Nicolacakis）表示，正如几个月前所表示的，区块链技术在多个行业都具有开放和颠覆性的潜力。从2016年揭开序幕，将会与Blockstream一起，跨越双方熟悉的领域来提供全方位的专业合作，为市场带来全面的区块链实施方案。

根据Blockstream的说法，PwC已经把该技术介绍给他们在美国、欧洲和亚洲的客户，并且正在探索金融和非金融领域的区块链用例。

弗勒补充说，PwC已经和比特币交易所共同实施了第一个行业侧链案例，称为Liquid，这已经提供了一个通过深入开发该项技术，为某个行业提供支持打开了大门。PwC为Blockstream打开了大门，并且为该领域带来全新的能力，许多企业能够探索因为区块链来临而带来的全新机遇。

PwC还选择了另一家区块链技术初创企业Eris，作为其区块链技术合作伙伴之一。

（三）安永

2016年3月，安永会计师事务所发布报告，专门研究作为数字化平台的区块链技术在保险业的应用。保险公司一直以来都不积极采用颠覆性创新技术，其创新战略唯一的目的就是维护客户和最大化企业利益。

目前这些企业纷纷开始探索区块链技术，认为该技术的去信任系统真正可以带来长期的战略性利益。因为它能提供安全去中心化的交易；精准及时的变动通知可以降低风险，增加资本机遇；降低运营成本；提高企业管理水平。

随着技术的进步，保险公司控制的活动应该慢慢转变为全新的数字化模型，其技术基础设施也就要相对升级以适应新的生态环境。新的分布式技术消除了保险公司的技术应用障碍，对现有金融模型构成一些威胁。区块链技术的潜能可以带来前所未有的行业透明度和可靠性。

对保险业而言，区块链主要提供了四大机遇：诈骗探测和风险预防、数字化的投诉管理、新的行业颠覆和资源分配、网络安全责任。

尽管区块链技术在保险业的应用前景很好，可是像所有新技术出现的初期阶段一样，该技术的可扩展性、实施技术以及与企业 and 政府机构的实际融合都引起了行业的担忧。

监管者担心的是关键基础设施还不完善，给现实技术融合带来隐患；区块链技术人员专业性不够，难以保障各方利益；损失控制机制标准化还在完善中。保险公司的主要担忧是，该技术的扩展性以及和现有系统的兼容性，风险管理、计划制订和时机把握。市场的主要担忧是，中心化基础设施的减少会带来高额的监管成本和复杂性；技术发展可能使强制性、规范性监管变得低效；市场需要弹性的审慎监管；欧盟委员会计划提高数据和隐私保护标准；消费者数据控制方式会改变。

总体来说，金融服务机构应该继续该技术探索 and 开发，创造适合行业发展的应用。安永也专门成立了核心团队，为企业家和保险公司挖掘提供机遇。

（四）麦肯锡

根据麦肯锡商务咨询公司的最新一篇报告，报告的标题为：《超越炒作：区块链在资本市场的发展》。该报告认为传统金融行业最终大规模采用区块链技术，将很有可能经过四个阶段。最终，区块链技术将会“深刻改变资本市场的面貌”，影响这个领域的商业模式、成本节省和

资金要求。麦肯锡报告声称，一旦社会采用区块链技术，社会将会获得可观的近期利益，加快资本市场的结算清算手续，同时降低金融机构需要保持的账本数量，并且确保审计跟踪更加精确。

但是，麦肯锡最主要的发现是，金融业必须协调一致，才能享受区块链带来的好处，这个结论支持了大银行所做的一些努力，也为分布式R3联合账本提供了支持。因为只有所有市场参与者、监管者和技术人员的通力合作，才能挖掘区块链技术的所有潜力，但这需要耗费时间。麦肯锡建议，区块链部署过程中的障碍，包括区块链数据不可逆的特性，可能会要求网络之类的参与者达成一个共识机制，以解决冲突。而且，麦肯锡确实提供了一份详细的路线图，介绍了不管遇到多少挑战，区块链如何完成转变，为金融机构提供了一扇窗，启发他们如何应对分布式金融技术的转变。

鉴于区块链的上述益处，麦肯锡认为这种技术的推出将历经4个阶段，分布式总账将第一次把所有法人实体的金融机构联合在一起。在这种情形下，每个公司的法人实体会成为分布式总账上的“节点和记账人”，之后借助技术的发展，机构将有机会与其既有平台“重新接线”。而随着时间的推移，设计问题可以内部解决或修改。第一步可以是如何把资产移入和移出封闭的区块链系统。从这一点来讲，区块链技术通过在银行中取代手动输入，可以达到扩大规模的目的，然后为技术提供“坚实的测试基础”。

麦肯锡认为，市场参与者的小规模网络，他们可以达成一致，共同遵守预定和转账的协议和标准，而且投资少，具有改良目前操作的潜力。此阶段过后，区块链技术将进入交易商经纪占主导地位的市场，最后被公开市场的购买者和销售者大规模采用。除此之外，区块链技术更有可能扩散的其他领域会是：金融资产证券化、贵金属、回购协议、联合银行债、产权保险和出售证券。而早先进入比特币领域的竞争者，他们当时专注的很多用途，将会需要更长的时间去发展。需要指出的是，

包括在支付系统的应用技术，随着时间的推移，以往在比特币市场上，基于经验的货币交易将会向外汇商务发展，因为比特币互换将会获得吸收现金储蓄的执照。此外，区块链技术在支付领域的应用将会超出目前的散户和小规模应用。

（五）埃森哲

1. 亚太投资报告

2015年11月，一份来自埃森哲的报告预测，亚太的金融机构和服务将会增加在云技术、移动钱包和区块链技术的投资。此外，亚太地区的互联网金融投资额将会是2015年的4倍。根据这份已经在11月3日公布的公告：“整个亚太地区在金融科技（互联网金融）方面的投资在2015年直线上升——2014年整年全部投资额约8.8亿美元，而到2015年9月投资额已经接近35亿美元。”

在这个趋势中最主要的是因为来自中国的投资额出现了大幅度的增长。除了有来自阿里巴巴控股集团的投资，来自移动支付和电子商务Paytm（印度最大的电子支付平台）的投资外，还有来自平安保险集团的P2P贷款和金融内容资产交易机构陆金所的投资。

埃森哲金融服务集团在东盟高级董事总经理及互联网金融创新实验室亚太执行官乔恩·奥拉维（Jon Allaway）表示，金融服务机构正在更多地采用云技术、移动钱包和区块链技术来重新定义自己的业务和运营模式。可以看到，来自银行互联网金融风投基金、孵化器和创业公司的投资正在增加。

此外，埃森哲澳大利亚兼新西兰高级董事总经理格雷格·卡罗尔（Greg Carroll）表示，澳大利亚的所有银行正在寻求将区块链技术整合

到他们自己系统的方式。这对于创新来说已经打开了大门，互联网金融初创公司也许能够在澳大利亚找到最好的机会。

来自埃森哲的研究显示，6%的董事会成员和全球最大银行中只有3%的首席执行官有技术方面经验。埃森哲最新的报告建议：金融机构和金融应该将重点放在区块链、云和网络安全方面，这是因为，作为一种独立的技术，区块链能够帮助银行、信用卡公司和清算企业进行合作，以创造更加安全、更快速的汇集和通过降低对手风险和交易延迟率来优化资金的使用。

2. 互联网金融创新实验室

2016年1月，埃森哲的2016年伦敦互联网金融创新实验室宣布，将会包括15个初创企业。在这15个企业中，Crowdaura将是唯一一个使用区块链技术的初创企业。Crowdaura能够使用区块链机制，通过众筹的方式来发行证券。

这些被选出的公司将会在未来12周内和埃森哲的员工一起工作，还有来自主流金融机构的管理人员也将会一起参与，其中包括美国银行、德意志银行和汇丰银行。

埃森哲金融服务部门主管理查德·伦波（Richard Lumb）说，公司“极其高兴”并迎接这些初创企业加入孵化器。他们提供一些非常令人振奋的创新，在超过30多个国家中已经获得了极其良好的记录，伦敦也是正在蓬勃发展的欧洲互联网金融社区的中心。

Crowdaura是第二个在埃森哲孵化器中工作，基于区块链技术的初创企业。在2015年夏天，在香港的汇款初创企业Bitspark也参与过埃森哲2015年亚太互联网金融创新实验室。

（六）兰德公司

兰德（RAND）公司是一家具有全球政策影响力的智库公司，它与国防和国土安全部门有着紧密联系，2016年1月，该公司发表了一篇名为《数字货币对国家安全之影响》的报告。该报告研究了非国家成员，包括恐怖分子和叛乱集团在正常的经济交易中通过使用数字货币，从而增强他们的政治和经济能力的可能性。

这篇报告由美国国防部部长办公室资助，整个研究过程是由兰德国防研究部门所辖的数字货币国防政策中心所主导，研究数字货币对国际和国内安全的影响。兰德国防研究部门是一家联邦政府资助的研究和发展中心，资助单位包括美国国防部部长、参谋长联席会议，统一作战指挥部、海军、海军陆战队、国防部门和国防情报局。

该报告认为，经过巴黎和圣博娜迪诺的一波恐怖袭击之后，可以预测数字货币将会成为恐怖分子策划犯罪活动的工具。就在巴黎恐怖袭击之后，有人就要求增加数字货币交易的控制，以防止恐怖分子借助数字货币绕过法币交易的监管和控制——或者完全禁止使用数字货币。

兰德更进一步建议，政府应使用先进的技术手段去主动破坏数字货币。这包括恐怖组织，也有其他和平利用数字货币的非政府机构，是对隐私和加密的全面战争。

根据兰德的 analysis，数字货币表现出数据存储的强大适应性，数据以高度分布的方式存储，而且很难被破坏。这可能会导致信息泄露（博客，社交平台、论坛、新闻网站），使国家干涉失灵。

报告中这样说道：“数字货币代表了去中心化网络服务的最后一步。特别是，历史趋势表明，发展一种适应性很强的公共网络密钥，报告将此定义为，不管国家机构拥有多么复杂的系统，都不能阻止简单的网络行动者获得持续的、稳定的网络服务。”

报告建议美国国防部门应摧毁去中心化数字货币，以防止全球任何人都史无前例地获取任何信息和交流服务。

兰德的研究者分析了基于区块链系统的去中心化特征，包括但不限于数字货币，其中比特币是一个为大众熟知的例子。但是不含货币应用的区块链技术，例如复杂的加密存储系统和去中心化网站的格式，以及交流服务，兰德认为它们也是威胁之一。事实上，比特币追捧度的增长带来了大众对复杂加密技术认知的提高。

报告这样认为，大众对区块链技术的认知提高了，人们就会提高对分布式共识和计算的复杂加密技术的认知，连风险资本家现在都在谈论计算机科学概念了，而之前这些概念仅限于学术圈子。

一个重要的考量就是，相对来说，公众对数字货币还是认识有限，也不太信任。但是当更多的人了解到去中心化，基于区块链系统的P2P等的长处时，包括价值存储、交易等，人们就会改变看法。事实上，数字货币变得越来越受大众欢迎，它不仅在发达国家被人追捧，在发展中国家也受人喜爱，那里恶劣的经济条件和低效的金融系统可能促使人们去接受一种非国家发行的数字货币，作为一种可靠的替代品。

因此，兰德的报告似乎在建议一次先发制人的打击，阻挠数字货币的发展，也许美国和其盟友最好的战略就是：瞄准数字货币增加接受度的特性，即匿名交易、安全和全球可用性。报告中同样给出了一些例子，说明如何对数字货币和基于区块链系统的其他应用实行打击。

与此同时，美国总统候选人希拉里·克林顿近期呼吁发起“类似曼哈顿计划”，加强加密通信的执法。全球其他国家政客也呼吁向加密技术开战，包括英国首相卡梅隆，他计划在英国推行强力加密技术禁止措施，该计划被一些高端网络活跃家嗤之以鼻。希拉里和兰德的建议区别在于，一家倾向于技术措施，另一家着重监管和禁令。

四、证券交易所的区块链案例分析

（一）纳斯达克证券交易所

1.代理投票系统

2015年10月，纳斯达克首席执行官鲍勃·格雷菲尔德（Bob Greifeld）宣布，交易所将会使用区块链技术管理代理投票系统。

简而言之，代理投票对于交易所而言，是一件非常重要且费事的工作，它需要由一系列在交易所上市的公司来处理。而通过这个全新方式，可以让股东在每年的股东大会上用手机进行投票，而不需要一定出席在周年大会上。这一举措首先将会在爱沙尼亚的纳斯达克市场进行测试。

格雷菲尔德说，纳斯达克打算把代理投票放在区块链提供的永不更改的公开账本上，这样人们就能够使用手机来操作（投票），并且记录可以永久保存。值得注意的是，纳斯达克一直非常支持这种区块链技术，因为这种技术看起来能够在更短的时间内让交易变得更加透明。

这个行动虽然出人意料但也是情理之中，因为早些时候，纳斯达克的首席信息官布拉德·彼得森（Brad Peterson）已经在这个主题上分享了他的观点，区块链技术在改变股票市场上具有非常大的潜力。这些语言来自全球资本市场上，仅次于纽约证券交易所的全球第二大交易所的纳斯达克高管，这对区块链技术而言算是一个极大的赞赏。

2.首个基于区块链的证券交易

2015年12月30日，纳斯达克宣布通过其基于区块链的平台完成了首个证券交易。在被称为Linq的基于区块链技术的平台上，完成了首个记录——这对于主流金融系统中将会是使用区块链技术的里程碑。

纳斯达克表示，Linq区块链账本已经把股票发行给一位不愿意透露姓名的私人投资者，通过去中心化账本证明了股份交易的可行性，而不再需要任何第三方中介或者清算。

2015年5月，纳斯达克宣布计划使用区块链技术大规模在企业内进行应用。纳斯达克表示不需要使用比特币，但是将会使用数字货币技术背后的技术。集团也决定使用区块链来改变交易完成的方式，而这将彻底改变市场运行的速度。

格雷菲尔德表示，相信这一交易的成功，标志着全球金融领域的一大进展，代表了区块链技术应用进入了一个开创性的时刻。

格雷菲尔德在12月初就表示，利用区块链技术，让管理传统实体证券转变成纯粹数字的方式。一旦不再需要传统世界中的繁文缛节，那么从区块链技术中受益的将不仅仅是我们的客户，而是更加广阔的全球资本市场……这个最初的区块链应用将会让传统烦琐的管理功能变得更加现代化、有序和安全。相对于传统人工保存台账的方式，将会具有压倒性的优势。

他指出，区块链网络将可以改变美国证券市场的交易时间，甚至可以改变整个金融行业处理交易事务的方式。这不仅有助于减少交易结算时间，还能够确保交易网络之间资金传输变得更快。

Linq是专门让私人企业发行债券和证券交易的平台。纳斯达克在2015年秋季参加了区块链公司Chain的3000万美元投资轮，其他主要投资者还包括Visa、花旗风投和第一资本。

纳斯达克的区块链平台已经正式上线，并且可以让私人企业使用，目前参与股权交易的企业包括区块链企业ChangeTip和PeerNova。

3.区块链发展还需要时间

2016年4月，纳斯达克主席和首席运营官阿德纳·弗里德曼（Adena Friedman）告诉媒体，区块链技术可以带来更快捷和更高效的交易结算。她解释说，区块链技术可以使纳斯达克等金融机构追踪任何资产的最终所有人。

纳斯达克为全球100多家交易所和清算所提供技术支持，与此同时，也在与客户谈论区块链技术及其潜在应用。在这个领域里，区块链技术的焦点主要是缩短结算时间、释放银行和清算所占用资本以及管理风险。假以时日，区块链技术一定会有发展的机遇，只是还需要些时间。

（二）纽约证券交易所

纽约证券交易所（New York Stock Exchange, NYSE）是最早表示对区块链技术感兴趣的公司之一，在2015年公布了两项声明，并且都与比特币有关。

2016年1月，NYSE投资比特币服务公司Coinbase。同时NYSE主席杰弗里·斯宾塞指出，这次投资，他们表示相信年轻人会积极使用数字货币，他们对价值交换有更进步的见解。

NYSE还会继续发布比特币价格指数，与Coindesk的比特币价格指数（Bitcoin Price Index, BPI）形成竞争之势。5月就会从Coinbase交易所平台的交易中获取相关数据。

（三）伦敦证券交易所

伦敦证券交易所（London Stock Exchange, LSE）也是交易后分布式总账工作组（Post-Trade Distributed Ledger Working Group）的创立者之一，在区块链技术试验中是最积极也最安静的。

这个工作组是继R3之后第一个出现的，它的成立表明，大型金融公司可以通过合作进行超越R3合作框架的区块链测试。此后一大批大型金融公司开始探索私人概念证明机制，同时进行的更大规模测试涉及了资本市场运营的参与方。而且LSE与Kouvola Innovation和日本交易所集团一样都是IBM区块链即服务平台的首批客户。

（四）澳洲证券交易所

1.升级CHESS系统

澳大利亚最主要证券交易所——澳洲证券交易所（Australian Securities Exchange, ASX）正在计划使用一套能够值得信赖的系统，来升级自己的证券清算系统，不排除会探索在新兴的区块链技术上来进行证券资金转移操作。

ASX已经和纳斯达克达成了协议，这家美国运营商将会负责升级悉尼集团的证券清算平台。纳斯达克将会参与项目的主要内容是，尝试创建一个可以运行的全新结算系统。

纳斯达克首席执行官鲍勃·格雷菲尔德在2016年2月告诉分析师，这个目前尚未宣布的协议将会让公司“季度订单总额有出色的表现”。这个消息是在ASX宣布它将会和DAH进行合作之后披露的，DAH是一家美国区块链技术服务提供商，将会为澳大利亚证券市场设计清算和结算系

统。

ASX有一个长期的计划，即准备在未来的三年里升级它的交易和交易后平台。纳斯达克和瑞典的Cinnober Financial Technology将会提供该系统的一部分组件。

DAH有可能会为ASX现有的结算系统升级CHESS（Clearing House Electronic Subregister System，结算所电子附属登记系统），这是一个证券结算服务，用于在对手方和法定股份持有者之间传输资金。

此举反映了全球交易、清算和结算运营者对于区块链技术潜力持续增长的兴趣，该技术能够为许多金融市场带来庞大的低成本计算能力。它能够让数字资产在交易对手方之间进行移动而不需要任何中央机构来负责记录交易。一个共享的数字公开账本能够持续被维护，确认所有参与链上的交易，防止被欺诈。

该技术的支持者称，该技术可以能够提高原有缓慢和低效的后端运作进度，并重塑交易和结算流程。然而，咨询机构Oliver Wyman和欧洲结算所Euroclear发布的一份报告争辩说，“目前需要克服的障碍是巨大的，而且最终的效果并不是很明朗”。这份报告称，建立市场运营者需要开发标准，要能实现现有支付手段及结算系统的所有能力，并且要满足现有的法规。它指出，许多区块链所鼓吹的优势，其实可以通过扩大类似于ASX的CHESS这种中央政权存管机构在市场中所扮演的角色来实现。

目前，ASX并没有承诺一定会使用区块链技术，用它来和现有系统内进行协同工作。ASX认为，“这需要能够让所有利益相关方都能受益，将会在2017年前对使用澳洲交易后技术做出最终决定”。

2.区块链技术的先驱者

澳大利亚连续多年的经济正增长，使国内缺乏创新动力和新的经济增长点，并且澳大利亚国民将国内经济增长的希望寄托于总理的更迭。这种复杂的国内形势，给创新企业带来机遇和挑战兼有的发展环境。显然，目前只有区块链技术拥有给澳大利亚注入新的发展动力的潜力。而国内对该技术的依赖，使得ASX首席执行官埃尔默·马克·库珀自信澳大利亚会成为区块链技术发展先驱。他表示区块链技术比以前任何技术更透明、更高效，他预言澳大利亚会成为使用区块链技术的先驱者。

2016年1月，ASX投资马斯特斯女士的公司数字资产控股有限公司支付了1490万美元，并获得了5%的股权。

埃尔默·马克·库珀在2016年3月被迫从ASX辞职，他曾经在澳洲金融评论商业峰会上表示，这项新技术每年能减少40亿~50亿美元运行股票市场开支。他认为，当今的股票市场，是一个非常顺序的流程。即使非常简单的交易也需要复杂的顺序流程。这些流程也有20多年了，如果能让每个人都踏上区块链的旅程，原来40亿~50亿美元也能缩小到很低的成本。在这个价值链中，ASX能开发创新、竞争和更好的服务。

ASX说它决定在埃尔默·马克·库珀继承人的领导下与数字资产公司合作此项目，并且2017年决定是否采取这项技术。

ASX副董事长彼德·希奥姆（Peter Hiom）说ASX是“首个表明我们要进行大规模的市场运作的交易所”，但是交易所不想“冒风险或与其他交易所不一样”，并且希望朝着共同协作的标准努力。

（五）韩国证券期货交易所

2016年3月，韩国唯一证券交易所Korea Exchange（KRX）宣布，它正用区块链技术开发一个柜面交易系统（OTC）。目前该研发项目正处于初期阶段，该平台可以帮助柜面交易客户减少交易费用。

虽然该平台正式发行之前还有很多准备工作，但这个平台有望可以简化场外经销商交易程序，降低交易成本，并协助寻找交易伙伴。这项举措使韩国证券交易所成为探索证券交易中区块链技术应用的公司之一。

2005年，韩国三大主流证券交易所合并，成立了韩国证券交易所。2015年，该交易所日股票交易量达到71亿美元。

（六）东京证券交易所

东京证券交易所（Tokyo Stock Exchange）是全球四大证券交易所之一，也是日本最重要的经济中枢。野村综合研究所是日本智库的代表，其影响力在日本甚至全球都很突出。野村综合研究所先后与野村证券和SBI Sumishin网络银行、东京证券交易所合作探索证券业区块链技术，下个阶段，SBI证券和三菱UFJ金融集团也会参与进来。

2016年4月，东京证券交易所运营商在为期一个月的区块链技术探索中与日本顶尖的智囊团合作。

这个试验项目由野村综合研究所（Nomura Research Institute, NRI）公布，该机构还透露日本交易所集团（Exchange Group）将该项目作为其区块链研究的一部分。作为IBM“区块链即服务”平台的早期用户，日本交易所集团一直在进行区块链应用试验。

NRI宣布在测试阶段，会在将区块链应用于证券市场之前，评估区块链的挑战和可用性。该项目尤其关注商业应用案例，其宗旨是开发证券市场应用专业区块链原型。NRI高级执行董事横手实

（Minoru Yokote）说，随着行业越来越关注区块链改善技术和行业运行的潜能，会致力于判定区块链技术应用于证券业未来应用程序的挑战和潜在利益。

2015年10月，NRI就已经开始区块链应用相关合作，当时该研究所宣布与野村证券和SBI Sumishin网上银行的合作关系。

（七）日本瑞穗金融集团

日本瑞穗金融集团（Mizuho）在2016年3月初，开始尝试基于区块链的试验项目，主要是聚焦跨境证券结算业务。该试验采用了开放资产协议，这项人们常用的彩色币协议增加了比特币没有的新功能。比特币可以通过该协议添加特殊标志，代表区块链中其他的资产。

日本IT巨头富士通及其研发部门富士通实验室参加了此次试验。试验时间为2015年12月至2016年2月，参与者说，区块链应用可以缩短交易后流程时间。

Mizuho公司表示，该系统中不断生成的包含贸易信息的区块按时间顺序组成区块链。这样，所有的信息就不能被篡改了。公司合作伙伴也承认，信息在公司间共享能缩短交易后流程时间。

Mizuho此次试验的目的是寻找缩短交易后流程时间和防止数据篡改的方法。目标是利用区块链技术建立一个低成本、低风险跨境证券结算系统。这个系统可以实时分享交易后流程中的交易信息数据并防止数据篡改，并且可以避免从头建立一个庞大的系统。

公司为该项目提供证券结算程序专业知识，富士通则负责开发相关的测试系统，富士通公司实验室部门负责进行试验。Mizuho还透露与IT咨询公司Cognizant合作开发区块链内部记录保存系统。

Mizuho和富士通不是唯一尝试利用区块链技术推动交易后结算流程的企业。2015年，伦敦交易所、法国兴业银行和瑞银集团已经开始探索区块链在该领域的应用。

Mt.Gox破产之前，Mizuho曾与该公司合作。Mizuho的区块链项目还包括与微软日本、区块链初创企业Currency Port及ISID（Information Services International-Dentsu）合作的银团贷款系统开发。

瑞穗的区块链项目还包括与微软日本、区块链初创企业Currency Port及ISID合作的银团贷款系统开发。该银行也是区块链财团R3的42家成员公司之一。

（八）多伦多证券交易所

多伦多证券交易所（Toronto Stock Exchange, TSX）是加拿大最大、北美洲第三大、世界第六大的证券交易所，由多伦多证券交易所集团（TSX Group, TSX: X）拥有及管理。在该交易所上市的公司种类繁多，主要来自加拿大和美国。交易所的总部设于多伦多，在加拿大其他主要城市如温哥华、蒙特利尔、温尼伯及卡尔加里均设有办事处。

TMX集团（TMX Group）是多伦多证券交易所的运营商，它也不曾透露其对区块链的兴趣。

然而该集团在2016年3月第一次公开表示，希望进行区块链技术探索，并且之前还雇用了以太坊项目联合创始人安东尼·约里奥（Anthony Di Iorio）作为项目首席数字官。下一代网络在3月发布生产模型以来，公众都把它看作最前沿的区块链应用。

安东尼·约里奥是加拿大比特币联盟执行董事、以太坊创始人，曾经组织了多伦多首个比特币峰会，可以称得上是北美数字货币业内非常知名的人物，并且多次来过中国参加过数字货币的峰会。多伦多证券交易所选择这样一位专家为公司在区块链技术领域开疆拓土，可见交易所对开发区块链应用的决心。

尽管多伦多证券交易所具体做法还不清楚，但能确定的是，它已经招募了一个区块链初创公司来搭建基于分布式总账的全新贸易结算系统。然而TMX集团仍表示其区块链技术战略还处于成型初期，可能很快就会进行技术测试。

（九）芝加哥商业交易所

芝加哥商业交易所（Chicago Mercantile Exchange, CME）是美国最大的期货交易所，也是世界上第二大买卖期货和期货期权合约的交易所。CME向投资者提供多项金融和农产品交易。自1898年成立以来，CME持续提供了一个拥有风险管理工具的市场，以保护投资者避免金融产品和有形商品价格变化所带来的风险，并使他们有机会从交易中获利。

CME是交易后分布式总账工作组（Post-Trade Distributed Ledger Working Group）的创立者之一，通过其投资公司CME Ventures积极地在该技术领域活动。

与其同行不同的是，CME采取了多元化的投资战略，投资的对象包括分布式总账初创企业Ripple、区块链投资集团Digital Currency Group和数字资产控股。这种投资组合使其具有跨领域行业活动的显著特征。

然而除此之外，CME没有公布更多的区块链技术研究方向和更大的行业战略。

（十）德意志证券交易所

德意志证券交易所（Deutsche Boerse）成立于1993年，总部设在德

国的法兰克福，在欧洲、亚洲和美国一些城市均设有代表处，是欧洲最活跃的证券交易市场之一。德意志证券交易所具备综合性一体化交易所职能，其使用的Xetra系统，是世界上流通性最强的现货市场全电子化交易平台。截至2010年12月，共有超过765家公司在德国证券交易所上市交易，总市值为1.4万亿美元。

德意志证券交易所是德国法兰克福证券交易所（Frankfurt Stock Exchange）的运营商，参加了2016年1月数字资产控股的6000万美元融资。

不同于ASX的是，它极少提及自己对该技术的支持。

2016年2月，该交易所少见的会见媒体，指出在进行多个区块链技术概念证明机制研究，只是还没有公布研究结果或发现。

（十一）迪拜多种商品中心

迪拜多种商品中心（Dubai Multi Commodities Centre, DMCC），是迪拜政府的战略倡导计划，目标是在迪拜建立全球商品交易市场。除了建立强大的有色宝石交易平台外，DMCC还承担了复兴阿拉伯珍珠文化的责任。为了满足这方面的需求，2007年，DMCC成立了专门的有色宝石和珍珠部门，不仅为买卖双方提供增加市场份额的服务，还搭建了国际贸易和业内服务的平台。

中东地区对区块链技术的探索极少，直至最近全球区块链委员会（Global Blockchain Council）透露，32个初创公司、金融公司、技术巨头组成的联盟开始探索区块链技术及其影响。

该联盟成员之一是迪拜多种商品交易中心，监管贵金属和其他有形商品的经济特区和商品中心。

2016年2月，DMCC宣布与比特币初创企业BitOasis合作进行区块链试验，探索怎样改善客户获取流程。

（十二）上海证券交易所

上海证券交易所（Shanghai Stock Exchange）创立于1990年11月26日，是中国大陆两所证券交易所之一，位于上海浦东新区。上海证券交易所总经理助理兼总工程师白硕在2016年3月接受媒体采访时，探讨了区块链技术在证券行业的应用。他认为区块链主要表现在以下几个层面：

首先，在业务层面，针对场外的、离散的、交易性能要求不高，或结算和支付效率要求相对要高的新业务来说，区块链技术是很有其存在和使用的必要的。但从场内的核心业务来看，区块链技术现在远远达不到其应用要求，也不适合区块链这类没有信任基础的场景。

其次，在组织治理层面，对这一层面的最大冲击，实际上是技术在引领业务，而不是技术成为业务的附庸。不管是传统的金融机构，还是新的金融机构，都要认识到这个问题。我们必须改变自身的态度，即使是传统金融机构也要考虑改变一下阵形。从“技术是业务的一种从属的关系，或者是服从的关系，我怎么说你怎么做的关系”，改变为“可不可以让技术在一定程度上冲在前面；让它们去发挥自己的想象力，发挥自己的创造性，看看哪些东西可以真正引领业务冲出来”，这与业务的推进没有关系。从组织治理层面上看，信息技术将成为组织变化的强大驱动因素，能够带领业务改变，促进业务发展。

最后，在技术层面，区块链技术应用到金融行业，其最核心的内容就是去中心化的一个防伪记录。如果无所谓是否去中心化，譬如某个机构运行得好好的，也没有受到任何的威胁，那区块链技术的应用显然就

不那么重要了。如果确实是有多方参与，且多方之间没有信任基础，但大家相信数学，相信算法，这种情况就比较好办。所以我们讲最核心的，对技术的关键就在这里，这个关键决定了它适用的场景。不管是效率问题还是安全问题，说到底就是一个去中心化，如果说去中心化不是十分必要的，没有这么大动力，那么大家也就不会对它过于在意。但从目前来看，大家应该是已经看到是有需求存在的，那么，区块链技术就是有其存在的必要的。

现在证券行业大量的场外业务、新业务，均具有一定的分散性和区域性。比如股权转让市场，每个地区自己的股权交易市场都不大。如果自己建区块链或私有链，并不是一个特别经济的做法，所以在这样的场景使用区块链，是特别值得关注的。

在分散性、区域性的业务特点下无可避免地会存在分散运营、分散建设的问题，即使不使用区块链的技术而使用云端，也会存在各自建设、各自运营、成本相对较高的问题，也会涉及各地区区域性业务的协调问题。如果使用区块链，有一个统一的区块链面向所有市场，或者说是有几个市场联盟性质的，大家就像使用一个公共设施一样，这样既能保证更好的加密性和安全属性，也比一般意义上云托管或者云迁移更让人放心。

希望区块链能给资源的集中，至少是IT技术设施集约化的使用能带来一些新的契机。

从实践进展来看，区块链技术在商业银行的应用大部分仍在构想和测试之中，距离在生活和生产中的运用还有很长的路，而要获得监管部门和市场的认可也面临不少困难。

通过区块链技术带动证券行业是一个契机，但并不是唯一的，至少是一个契机，因为大家都有各种不放心，有各种一个本位的考虑。如果使用传统的IT技术，并不能让他们放心，打消顾虑，但是如果我们使用

区块链，如果宣传到位，从技术上讲，其实应该是可以打消顾虑的。

目前对区块链技术是以研究、跟踪为主。经过评估，目前场内的核心业务不适合使用区块链技术。至于其他的业务，目前是一边做评估，一边跟踪，以评估为主。

当前，面临的问题还很多。第一，区块链自身的效率问题。基于我们的业务情况，我们很重视效率问题。作为全国性机构，自身影响大，使用的人多了，交易也多，效率上如果支持不了，肯定是一个问题。第二，如果是私有链，是采用工作量证明，还是采用又耗能且不一定有很大必要的事情，重点考虑。技术本身也需要改造，改造成适合我们的相对封闭的用户群，而不是像公有链那样敞开的用户群，场景是不一样的。这一点也会特别关注。

像上海证券交易所这样有影响力的单位，开展一些推广面比较大的业务，到底适不适合也存在一定的问题。如果说有一定的采用价值，可能要评估需要进行什么样的改造，而不是简单地照搬。如果在公有链基础上看肯定是不行的，从各个方面看也还不是特别令人放心；如果是私有链上，则要看做什么样的改造可以使它的效率更高，这也是要有一些功课要做的。

目前能看到的是核心业务及高流动性的业务采用区块链是没有什么必要的。但是一些离散化的场外业务，甚至是国际业务，采用区块链是有一定可能性的，当然这里有不同的做法。简单地做一个登记，就是记账，这是一种做法，如果里边真的有数字货币或者跟法币挂钩的货币，这就涉及另一个问题，即央行的问题。

大家都面临着国家的货币政策方向的问题，所以区块链有两种用法，一种是不涉及货币，只做登记和结算，这种虚拟资产的搬家还是可以的。有合适的应用场景，可以尝试着做起来，前景还是光明的。另一种是凡涉及货币的，那可能最后就是取决于央行。

如果不涉及货币的问题，5年或者10年以后，是否可以看到区块链技术在证券行业的应用，这个是有变数的。目前的这种做法，无论是公有链证明还是权益证明，用一个私链，比如像我们这个登记公司的私链，它到底能怎么用，目前还不是很确定，这是第一点。它是不是能够原封不动地拿到我们这样的场景来，还是说要进行什么样的改造？如果是根本性的改造，安全性是不是经过了足够时间的考验？是不是可以马上进入生产？5年肯定是不乐观的。大家现在都很积极地在探讨，在研究、调研、评估。核心的交易和结算的生产机构，要是区块链进来，5年之内肯定是不乐观的。但是区域性的、离散化的、低流动性的、场外的，有合适的场景，肯定是可以，5年之内应该是可以见到的。

区块链技术的发展在全球范围内尚处于早期阶段，各种技术方案、应用场景和商业模式等还需要进一步的探索和完善，特别是在我国，区块链作为一个全新的概念和理论，人们的认知、研究和实践刚刚起步，要想在这一领域弯道超车，赶超先进，引领世界，还需要足够的重视、更多的投入，需要理论研究者、网络技术者、金融从业者，以及政府监管部门的积极投入、勇于探索 and 不断创新。

第七章 全球区块链投融资分析

由于区块链技术正在经历快速发展，数十亿美元正在快速注入区块链相关企业中，于是在行业中发生了大量的投资和市场活动——自从2009年以来，大约有13亿美元已经投入到该行业中。这13亿美元的投资，主要还是集中在与比特币相关的企业，特别是和挖矿相关的企业，如21 Inc或是BitFury，抑或是基础设施相关的企业，如Blockchain、Blockstream、Ripple和以太坊等，很明显这是行业初期发展的特征，而大量的资本投入必然可以促进行业快速成长。而由于比特币相关企业发展最早，所以相对而言更容易获得投资。但随着资本市场将注意力放到区块链技术上，有更多的小型区块链初创企业有待于发掘。

计算机硬件公司21 Inc目前似乎处于领先地位，自从2013年以来已经收到1.21亿美元的投资，紧接着就是Coinbase，它获得了1.05亿美元的投资。

在过去的几年时间里，区块链行业中的投资金额一直在成倍增加，目前获得资金最多的20个企业，大多数都是在2011年之后成立的。但是，目前只有BitFury、Circle和Coinbase完成了第三轮融资，其中大部分公司还处于早期几轮融资阶段，表明未来投资的机会才刚刚开始。

一、主要的投资领域

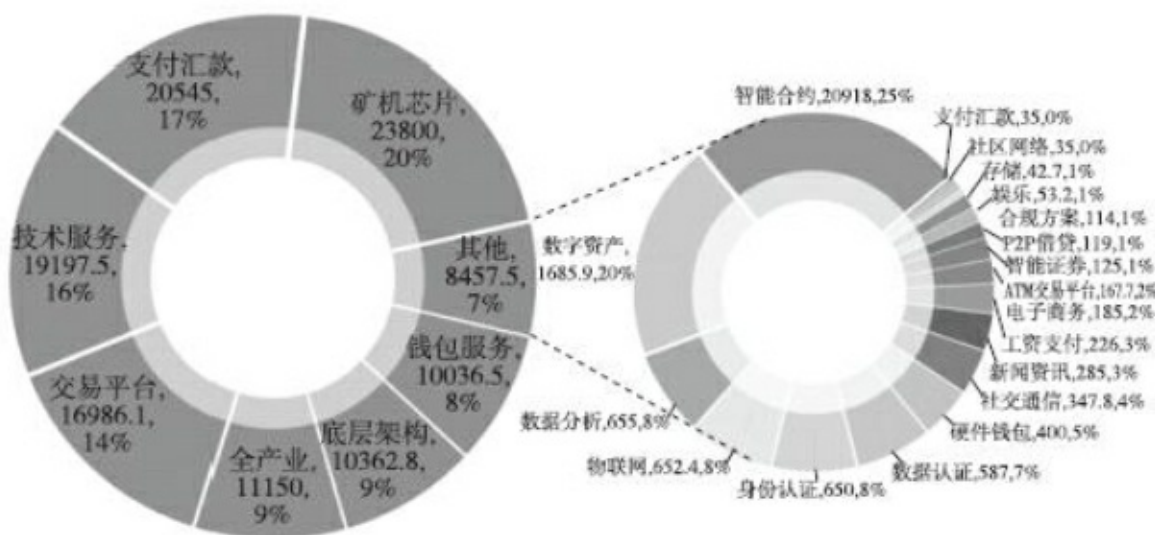


图7.1 2013年至2016年4月全球区块链行业投融资项目类型分析

从图7.1可以看出，目前最主要的投资还是集中在和比特币相关的领域，比如矿机芯片、交易平台、支付汇款、钱包服务领域。相对而言，这些领域更加成熟，参与的企业更多，创立的时间也更久。

其中，挖矿领域是一个投资相对最多的行业，图7.1主要都是统计在欧美矿机行业的投资行为。但是，根据实际情况来看，考虑到在中国大陆地区有更多的矿机厂商和矿场投入，应该有更加集中的资金投入。但是中国地区的这些投资信息大多数都没有公布出来，因此无法知道真实的投资情况。不仅国内如此，大多数矿机和矿场的资金投入，主要都是来自自筹资金，而目前大陆地区比特币算力占有全球总算力的70%，所以也可以推断出矿机和芯片之类的总投资额，至少是在目前统计数据

除了这些之外，其他领域有着更多的细分情况，其中包括智能合约、数字自资产、数据分析、物联网、身份认证、数据认证、硬件钱包、社交通信等。这些细分领域，许多都是基于比特币区块链，或者包括以太坊在内的其他区块链之上的应用，所以相对来说都是一些早期项目，更多的是在种子轮或者天使轮的投资。

二、不同地区/国家的投资差异

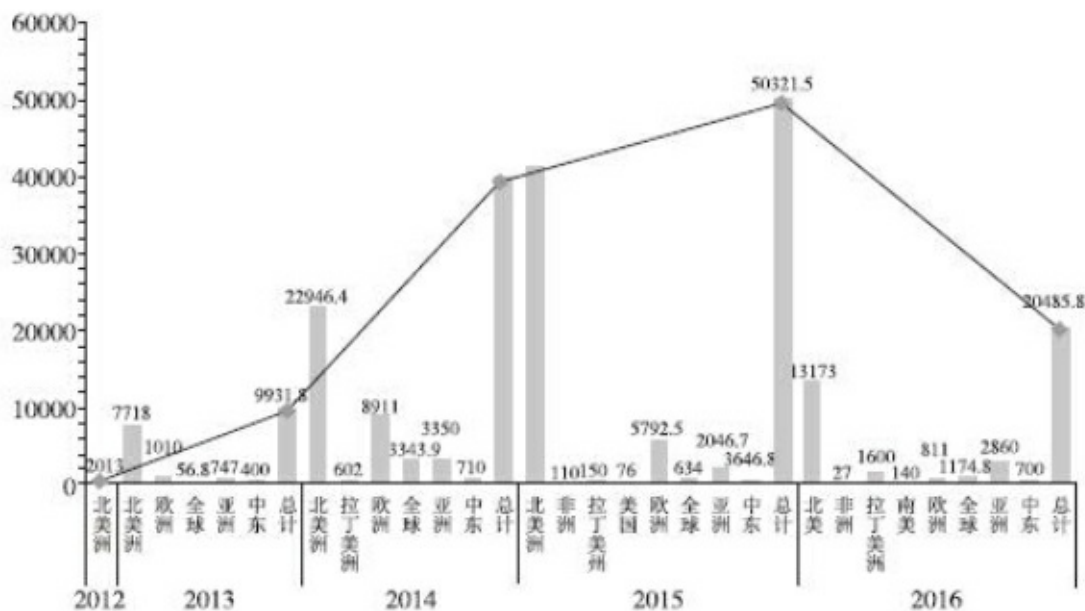


图7.2 2013年至2016年4月全球区块链行业投融资项目类型分析

在图7.2我们可以看出，目前统计的投资数据呈现一个线性增长的趋势。在2012年，几乎没有太多的公开投资情况出现，到2015年，已经出现了众多的投资事件，而且覆盖在区块链行业的多个领域。

同时能够发现，在每年的投资中，北美洲占据了主要的份额，有大量的投资都是集中在北美洲，而欧洲紧随其后，然后才是亚洲。造成这样比例的原因，主要还是因为区块链作为IT技术和互联网行业的一部分，北美洲在这方面有着较丰富的技术和人才积累。主要的理论建立和技术方案基本都是北美地区的技术人员提出，并且着手实施的。在这方面，其他地区要远远落后于北美地区。

从比特币到区块链，目前其实还处于一个初级的发展阶段，主要还

是集中在技术的基础架构建设中。而纵观整个IT技术的发展史，在基础架构领域，基本都是以欧美为主的。无论是UNIX、DOS、Windows、Linux还是Android，这些基础操作系统或者数据库系统，都需要有对IT技术有着深刻的远见和庞大的资金投入，以及大规模技术基础才能够进行开发。而亚洲地区在这一领域始终没有太多的话语权。到了比特币和区块链阶段，无论是基础理论还是最早原型设计，也都是在欧美开始的，因此，似乎也没有理由认为亚洲能够突然在这方面有机会全面超越欧美地区。

但是，必须要指出一点的是，在早期阶段，亚洲大多数国家对于比特币并不持有友好的态度。中国曾明文规定，禁止所有金融机构和支付机构开展比特币等数字货币相关业务。而早期全球最大的比特币交易所Mt.Gox在日本因为遭受黑客攻击而倒闭，并因此产生了一系列诉讼行为，所以日本政府对于数字货币的态度也一直非常冷淡，而且希望对此进行严格的监管。在未来政策上的态度不明确，必然会造成投资事件和金额远远低于正常的情况，或者也造成有许多投资事件不愿意公开披露。

正如前面所指出的中国大陆地区，在比特币矿机和芯片方面的投资情况，如果把这些从未披露的投资数据都计算在内，也许也不会低于欧洲方面的投资数据。

截至2016年5月，2016年的投资数额已经超过了2015年全年投资数额的一半，因此2016年整年的投资数额超过2015年应该是大概率事件。有理由相信，区块链行业相关的投资将在未来变得越来越频繁。

但是有个有趣的现象是，尽管从2015年下半年开始，“区块链”概念被视为在未来会获得越来越多的重视，许多相关会议和金融媒体都在密集地讨论其可能带来的颠覆式影响，甚至认为“区块链”技术已经被炒作过度，甚至可能有泡沫产生。但是从投资数据来看，并没有出现极大幅度的增长，完全是呈现出一个线性增长方式。从这一点来看，无论“区

区块链”这个概念被如何热炒，投资数据完全表现的是一种行业初级发展的特征，没有任何出现指数级增长的“泡沫”现象。

考虑到区块链技术在未来多个行业的发展可能性还具有极大的不确定性，而目前更多集中在底层架构的探索中，许多投资机构抱着观望的态度，希望能够等待局势更加明朗后再大举进入。

不同于在互联网发展早期，许多新的技术和创新都是初创公司开始，许多大型公司都是扮演投资者和并购者的角色。由于区块链要获得大规模应用，最容易的方式不是推翻目前所有的金融场景，而是帮助现有金融场景降低成本或者提高效率。因此许多参与区块链的研究和开发，都是在大型金融机构内部进行的。因为只有他们有更加合适的应用场景，并且明白自己的需求和痛点所在，但也因为这个原因，他们的具体进展和投入都没有对外公开，所以这方面的许多数据无法从公开渠道中获得。

所以，根据目前的线性增长趋势来判断，类似于1995~1996年的互联网投资情况，距离2000年的全球互联网泡沫的高峰形态相去甚远。完全可以认为区块链行业投资在未来还有巨大的上升空间。

三、不同年度的投资重点差异

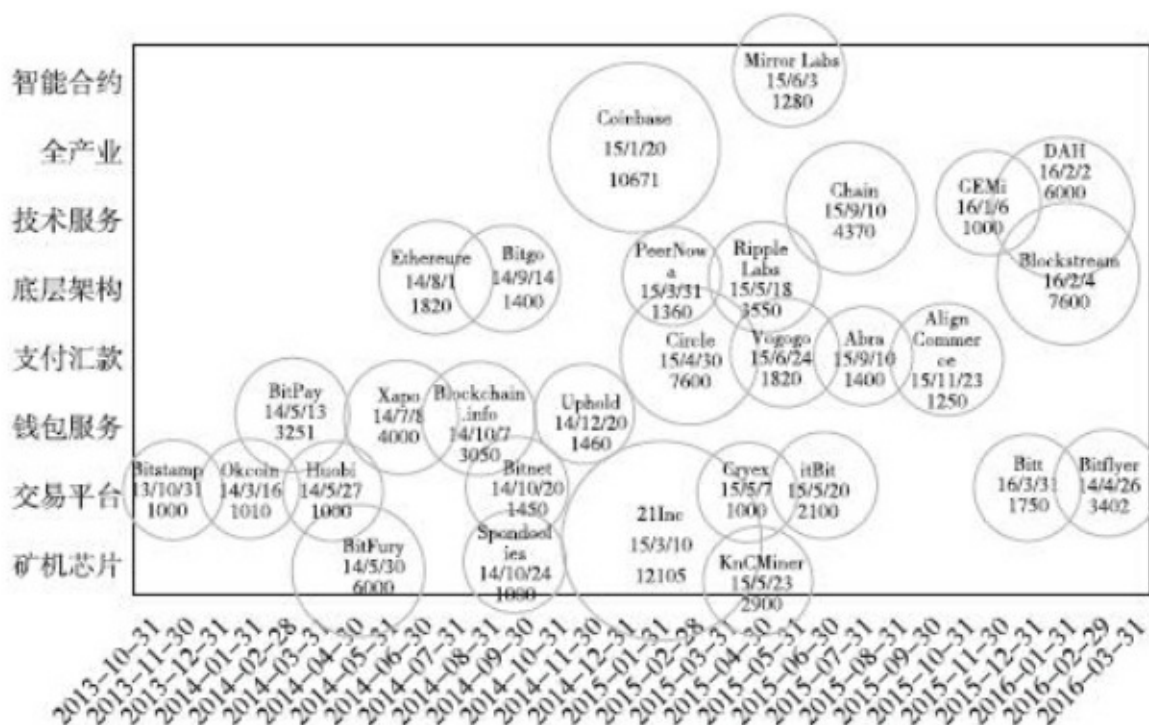


图7.3 2013年至2016年4月融资额超过1000万美元项目一览表

图7.3是全球融资额超过1000万美元的区块链项目，分别在行业类型和融资的时间节点上的分布图。从图中可以看到，投资机构对于区块链在不同时间和不同领域的兴趣点。

可以发现投资者在早期更多的关注矿机芯片和钱包服务，显然这都是和比特币密切相关的，而从2015年之后，开始把关注点开始转移到支付汇款、底层架构和技术服务上。这本身说明，投资者开始不再把所有的投资重点放在比特币上，而是开始重点建设整个生态环境。

有趣的是，对于交易平台的投资始终比较持续，可能不论未来区块

链是何种走向，哪些区块链项目将会崛起，交易所始终会是打通数字货币和法币之间的桥梁。区块链行业本身在快速发展中，体量也變得越来越大，必然会需要更多类似于桥梁这样的配套措施。所以，相信在未来还会出现更多的数字货币交易所。

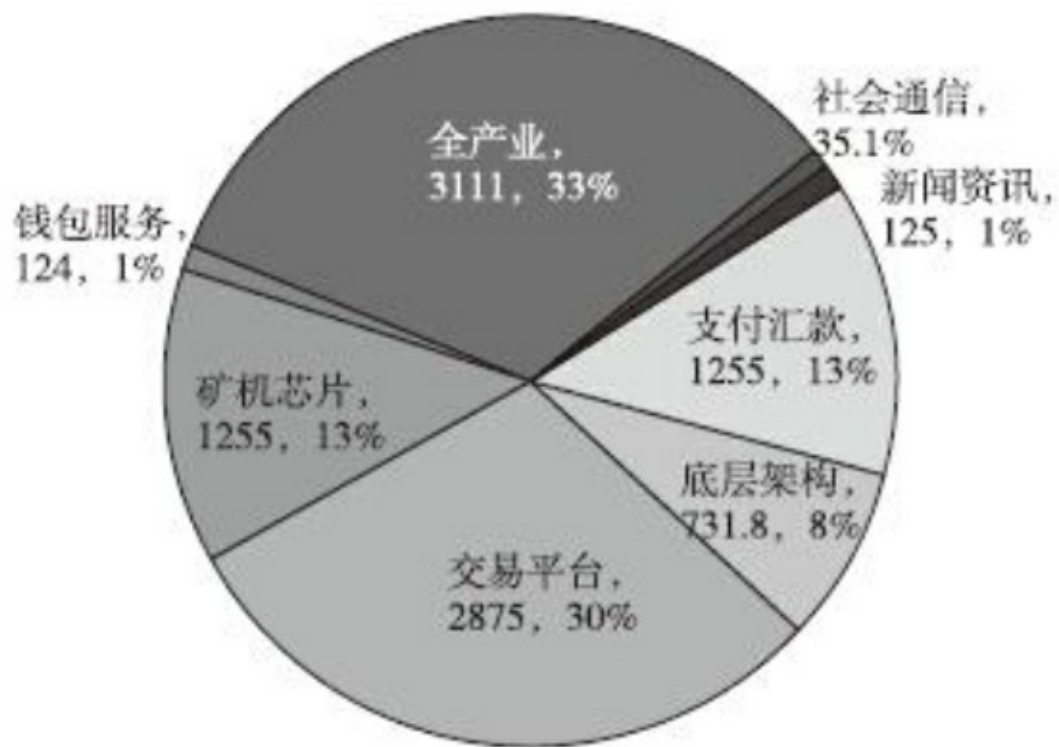


图7.4 2013年度区块链项目投资类型分析

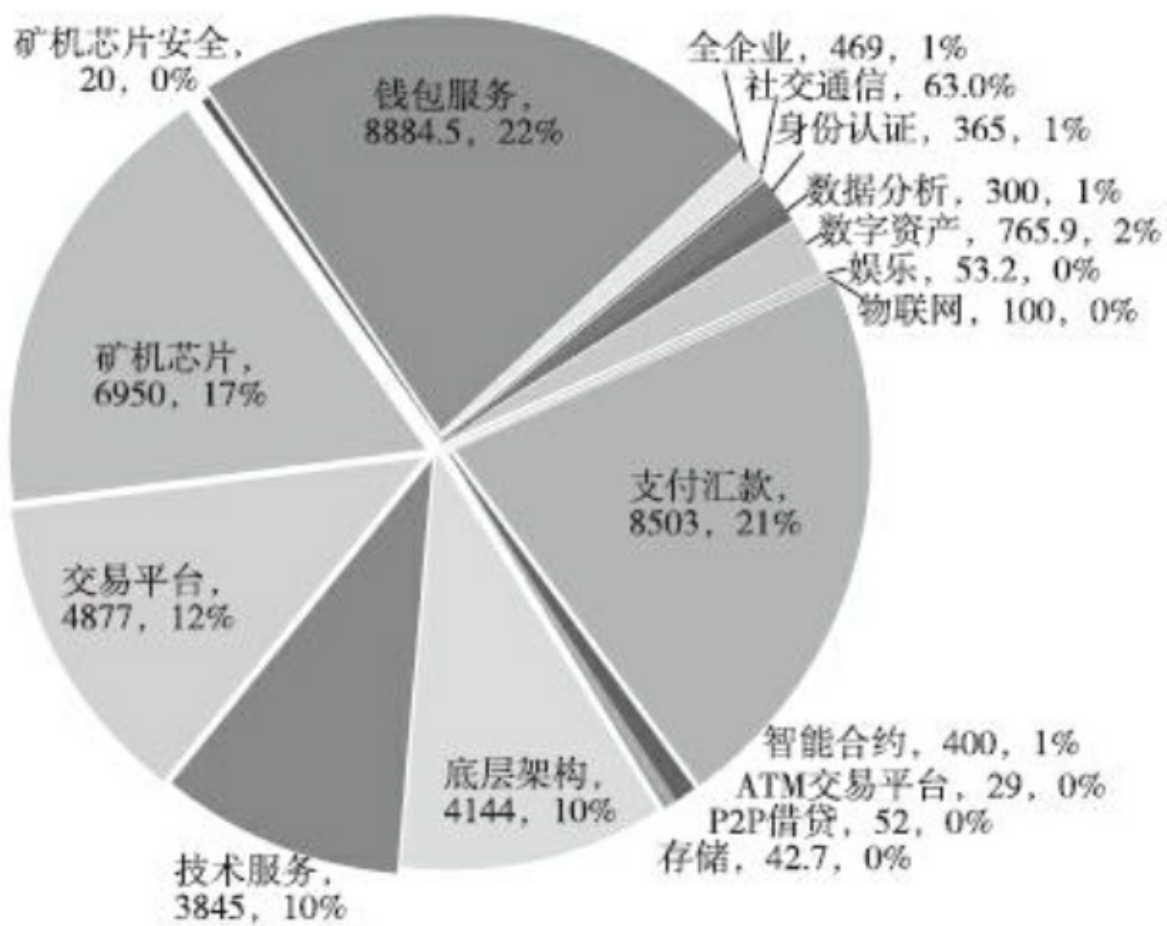


图7.5 2014年度区块链项目投资类型分析

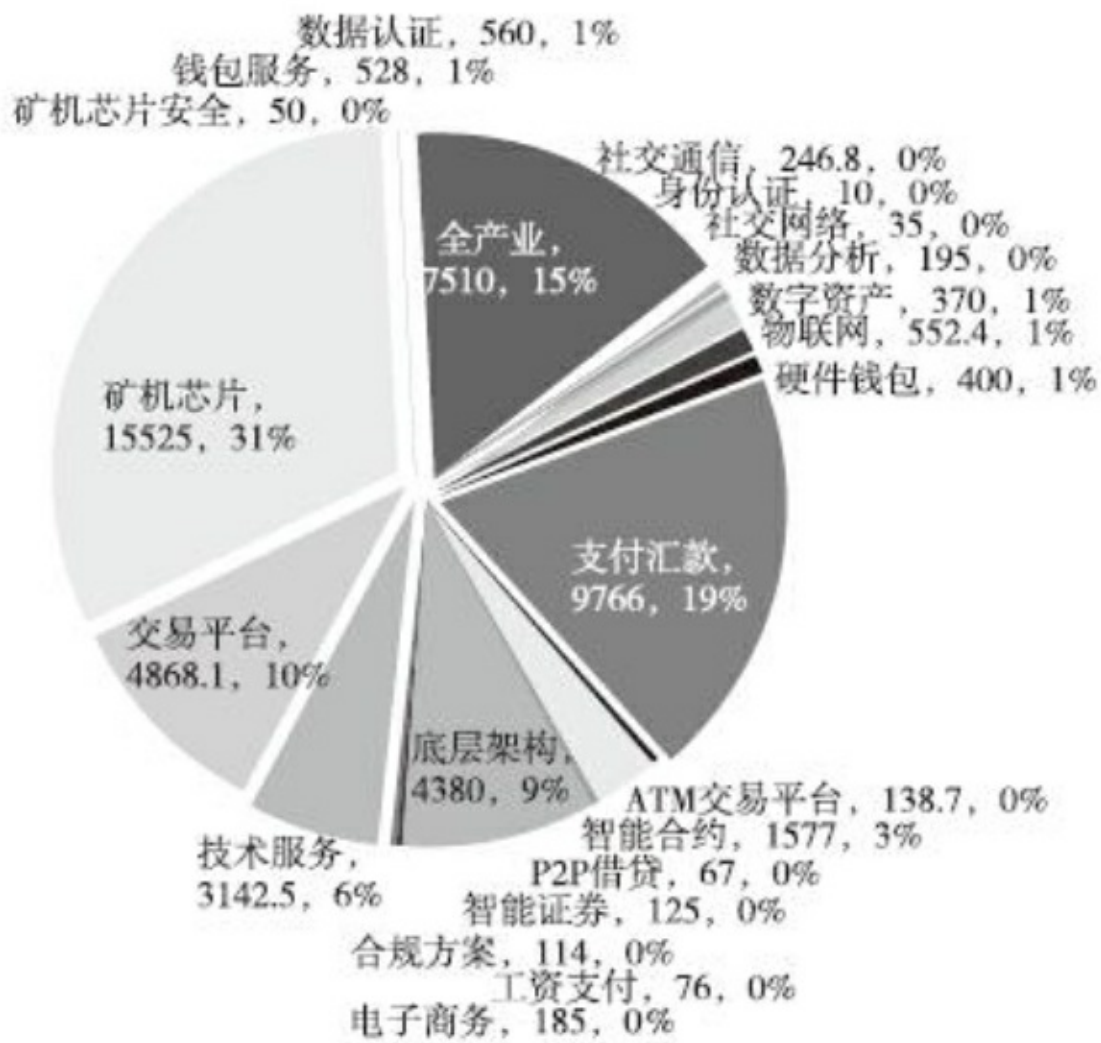


图7.6 2015年度区块链项目投资类型分析

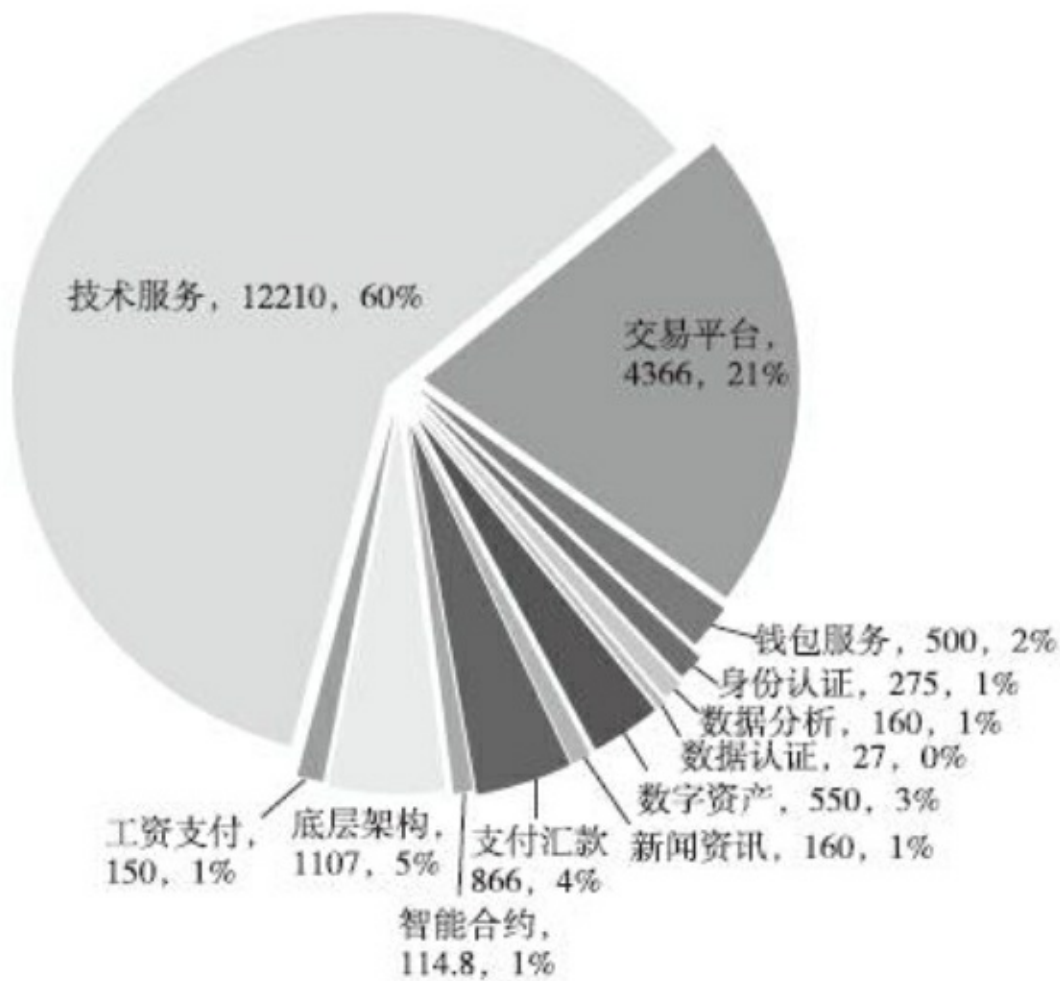


图7.7 2016年5月前区块链项目投资类型分析

通过对不同年度的投资类型的分析，我们也可以看出随着时间的推移，投资重点的确发生了不小的变化。很显然，从比特币时期的投资矿机和钱包之类，开始更多地形成以区块链技术为核心的完整生态系统。

另外一个比较明显的特征是，行业细分类型开始越来越多，会有很多围绕着核心生态系统的衍生产也开始逐渐诞生。尽管这些细分行业还十分弱小，但是能够看出，区块链已经在更多的细分行业获得了资本市场的认可。

四、ICO方式的崛起

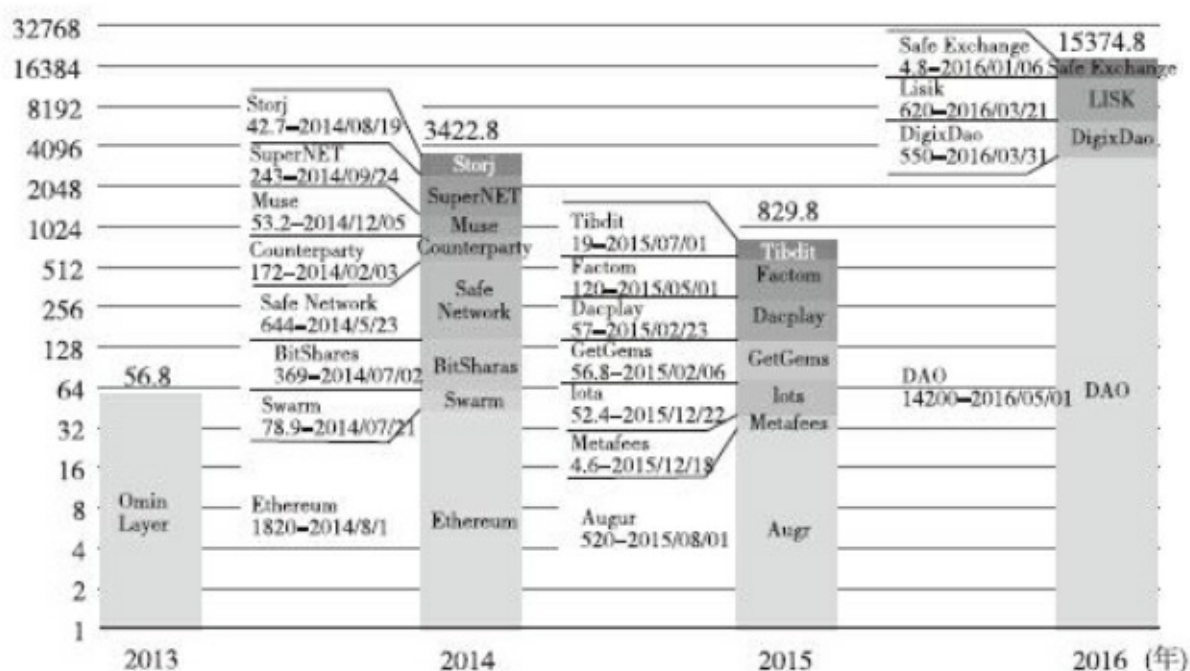


图7.8 2013年至2016年4月区块链项目ICO（Initial Coin Offering）融资情况

图7.8是专门分析区块链ICO融资情况。ICO融资是区块链行业的一个独有的融资方式，并且很有可能会改变整个区块链甚至是其他行业的融资情况。因此，是值得进行深入研究和探索的。

所谓ICO是指通过发行代币（Coin或者Token）的方式来进行融资的。有许多区块链项目是以DAO的形式来展现（关于DAO的定义和运作方式，请参见DAO章节），所以它们可以发行代币来代表该项目的一些收益权或者股份。每个项目根据投资者投资金额比例来发行相应的代币给投资者，而这些代币往往可以在一些数字货币的交易所里进行交

易。

无论是从其名称还是其实际运作方式，都很容易让大家联想到IPO。事实上，这非常类似于初次股票的发行，投资者支付一定的费用认购自己相应的份额，而这部分份额以某种凭证的方式，可以在交易市场进行自由交易。可能主要也是考虑法律方面的原因，这些区块链项目不愿意称相应的份额为股份（Shares），而是称为代币（Coin），也刻意回避了IPO的说法。

尽管在过去的几年中，众筹（Crowdfunding）也曾经非常热闹，但是众筹的方式很难让投资者随意退出。而ICO，能够让那些投资者几乎在每一分钟都可以进行交易，这让投资者持有的份额具有极好的流动性，这些流动性也会使项目估值产生更高的溢价。

此外，类似于像传统VC（风险投资）和PE（私募股权投资）这样的投资机构，他们往往对于投资项目具有很大的话语权，会极大地左右创始团队对于项目的ICO推进路线，而在ICO中，创始团队似乎具有更大的话语权，大多数投资者只能选择买入或者卖出他们的份额，而无法直接干涉创始团队的工作。当然，这也可能造成创始团队有可能对资金的滥用和欺诈行为，但是创始团队如果想要以更高的价格来抛售自己所持有的份额，就必须更加努力地工作，让整个市场认为该项目在未来有着更高的价值。

我们在前文指出，区块链行业投资的年度总额是以线性的方式在增长，而从图7.8中的纵坐标可以看出，这里使用了对数坐标，这说明ICO的总金额在快速增加，有越来越多的区块链项目开始使用ICO的方式进行筹资，这也是区块链行业和其他新兴行业最大的区别。传统的新兴行业往往通过VC和PE来进行筹资，而区块链行业却增加了ICO这种方式。这可以算是区块链行业一种非常独特的现象，让区块链行业融资形成了一种全新的生态环境。在不接触传统投资机构的情况下，完全以自给自足的方式进行融资，并且能够完成整个行业技术的快速迭代。

类似于以太坊这样的区块链项目，往往都是通过ICO的方式进行融资的。不仅可以在短期内募集到大量的资金，而且可以避开许多的法律问题。特别是ICO的方式是可以不需要法律主体的，而很多区块链项目本身就处于法律的灰色地带，因此越来越多的区块链项目开始采用了ICO方式来筹集资金。

ICO另外一个不同于传统融资方式的特点是，初创团队往往并不会留下很多的权益份额，而是把大部分权益份额全部让给参与众筹的投资者。这 and 传统VC，或者PE有非常大的区别。熟悉传统融资过程的专业人士肯定知道，专业的VC、PE进行投资时，往往不会占有大部分股份，而只是获得少量股份。他们还是希望初创团队占有大部分股份，这样初创团队才有足够的动力来开创全新的事业。但是在ICO中，我们会发现初创团队更愿意把大部分权益份额让给投资者。这是一个非常值得探讨的现象。

这在一定程度上不排除受到比特币的影响，因为比特币本身是由一个匿名的开发者创立的，这个自称为“中本聪”的匿名开发者并没有为自己谋求许多的权益，也从未要求自己在比特币的全部份额中占有一定的比例。尽管在开始阶段，“中本聪”自己也“挖”了不少比特币，但是他从未动用过自己的比特币，也就没有从中获得任何的私利，甚至在盛传他将被推举提名诺贝尔经济学奖的时候，他也没有表明过自己的身份，看来也没有贪图过“虚名”，就是这样一个完全不为名利的人，激励了许多人希望能够效仿“中本聪”无私的精神。

当然，精神激励并不是一个主要的因素，更多的原因可能来自市场机制。由于区块链本身是一个大规模协作工具，这注定区块链项目必须有大量的用户参与才能够让项目蓬勃发展起来。而只有项目得到发展，那些开发者手中持有的权益才能够变现。而参与ICO的投资者如果发现初创团队本身并没有持有太多的筹码，也许会更加愿意参与众筹，因为这样也许不会让投资者感觉是纯粹在为初创团队打工。

所以，从经济学角度来看，那些初创团队能够意识到，如果项目发展不起来，手上持有再多的筹码也没有意义。只要项目能够发展起来，即使很少的一部分，也能获得不菲的回报。因此，他们通过持有较少的权益份额，而出让更多的权益份额，能够让更多的人有意愿参与到项目中。而那些早期有参与项目的投资者，在后来为了让自己所持有的代币能够增值，也会自动成为项目的义务推广者，这对于项目未来是否成功有着巨大的推动作用。所以也让更多的项目创始人选择这种共赢的方式进行ICO。

2016年5月，ICO的方式达到一个全新的阶段。一个基于区块链，项目名称为DAO的去中心化自治基金在公开众筹中募集了约1.5亿美元的资金，打破了全球所有的众筹纪录。这个去中心化自治基金是没有中心化的管理机构，也没有传统的企业实体，每个人投资的人集体参与决策。尽管整个项目在众筹阶段饱受争议，有很多人质疑这种集体决策的方式来进行投资，其结果是否能够带来足够的回报。同时，全球主要的金融媒体，连篇累牍地发表文章探讨DAO可能带来的法律问题，以及未来对于全球融资业态的影响。但必须承认，这是一种非常大胆的尝试，并且DAO项目的成功记录，吸引了更多的人开始了解ICO这种方式。

从目前透露的消息来看，未来还会有大量的全新区块链项目会采用ICO的方式来募集资金，而募集资金的数量也会急剧增长。总体来说，项目增长的速度可能会低于关注人群增长的速度，而所有的ICO基本都是面向全球投资者的。所以未来可能ICO的众筹资金数量还会屡创新高。并且，不排除区块链之外的其他行业也会开始逐渐关注这个奇特的方式。不过，并不是所有的项目都适合使用ICO方式。顾名思义，采用ICO方式的前提是，该项目应该会内置代币，而这个代币必须能够代表该项目的部分权益。所以，未来ICO能否在更多的领域获得应用，是一个非常值得观察的现象。

五、总结

需要指出的是，我们数据统计资料都是来自互联网公开的信息，可以明确的是还有许多尚未公开的投资事件已经或者正在发生。比特币和区块链行业有一个有别于其他行业的特点，就是在2015年之前，比特币在许多国家都是一个相对敏感的领域，所以有许多的投资事件从未披露过。很多个人或者投资机构并不希望别人知道自己和这方面有关的企业有投资关系。

截至2016年5月，比特币总市值已经达到80多亿美元，而主要的区块链项目总市值达到100多亿美元，因此有理由相信，在这方面的实际投资可能会远远超过我们能统计到的数额。

关于全球主要区块链投资项目的详细数据请参见表7.1。

表7.1 全球主要区块链投资项目

项目	类型	国家	时间	资金	融资类型	情况
21 Inc (21c6)	矿机 芯片	美国	2015/03/10	11600	C 轮	Andreessen Horowitz、RRE Ventures、来自中国的私募股权公司 Yuan Capital、芯片制造商高通公司 (Qualcomm)，其他投资者包括 Khosla Ventures、Data Collective、PayPal 联合创始人 Peter Thiel、Max Levchin、eBay 公司联合创始人 Jeff Skoll、Dropbox 公司首席执行官 Drew Houston、Expedia 首席执行官 Dara Khosrowshahi、Zynga 公司联合创始人 Mark Pincus
			2013/11/17	505	A 轮	Individual Investors
Abra	支付 汇款	美国	2014/08/01	200	种子轮	Scott and Cyan Banister
			2015/09/10	1200	A 轮	Arbor Ventures、RRE Ventures 和 First Round Capital，还包括美国运通和印度塔塔集团名誉主席 Ratan Tata
Airbitz	钱包 服务	美国	2015/01/12	3	种子轮	Plug and Play Tech Center
			2015/05/06	45	种子轮	Block26

Align Commerce	支付 汇款	美国	2015/11/23	1250	A 轮	领投方为硅谷传奇投资公司 KPCB, 跟投方包括 Digital Currency Group、FS Venture Capital、Pantera Capital、Recruit Ventures Partners 以及硅谷银行的投资部门 SVB Ventures
AlphaPoint	技术 服务	美国	2014/10/17	135	种子轮	Ben Franklin Technology Partners、Robin Hood Ventures、Scott Becker、Gabriel Weinberg
Anycoin Direct	交易 平台	荷兰	2015/01/21	56	种子轮	未知

项目	类型	国家	时间	资金	融资类型	情况
Armory Technologies	钱包服务	美国	2013/09/01	60	种子轮	Trace Mayer、Jim Smith、Kevin Bombino、Individual Investors
Ascribe	数据认证	德国	2015/06/24	200	种子轮	Earlybird Venture Capital、Digital Currency Group、Freelands Ventures、angel investors
Augur	智能合约	全球	2015/08/01	520	众筹	
Avalon Clones	挖矿	美国	2013/07/22	300	A 轮	N/A
Bex. io / Spawngrid	交易平台	加拿大	2013/12/01	50	种子轮	Cross Pacific Capital Partners, Individual Investors
Bitbond	P2P 借贷	德国	2015/05/20	67	种子轮	Point Nine Capital, Christian Vollmann
			2014/08/13	27	种子轮	Point Nine Capital, Nelson Holzner
Bitex. la	交易平台	阿根廷	2014/05/30	200	A 轮	未知 UK-based investor
			2014/01/15	200	种子轮	未知
Bitflyer	交易平台	日本	2014/07/22	160	种子轮	Unnamed Japan-based venture capital firm
			2014/10/10	24	种子轮	Bitcoin Opportunity Corp.
			2015/01/28	110	A 轮	Bitcoin Opportunity Corp、RSP Fund No.5、GMO Venture Partners

项目	类型	国家	时间	资金	融资类型	情况
Bitflyer	交易平台	日本	2015/08/12	408	B 轮	三菱 UFJ 金融集团旗下的三菱 UFJ 资本有限公司 (Mitsubishi UFJ Capital Co., Ltd.)、日本电通集团旗下的风投公司电通数码控股公司 (Dentsu Digital Holdings, Inc.)、日经集团旗下的财经信息提供商 QUICK 公司 (QUICK Corp.)、三井住友保险公司旗下的风投公司 (MITSUI SUMITOMO INSURANCE Venture Capital Co., Ltd.)、创业投资有限公司 (Venture Labo Investment Co., Ltd.) 等
			2016/04/26	2700	C 轮	Venture Labo Investment, SBI Investment
BitFury	挖矿	荷兰	2015/07/09	2000	C 轮	The Georgian Co-Investment Fund、DRW Venture Capital、iTech Capital
			2014/10/09	2000	B 轮	Bill Tai, Bob Dykes, Georgian Co-Investment Fund, Lars Rasmussen
			2014/05/30	2000	A 轮	Binary Financial、Crypto Currency Partners、Georgian Co-Investment Fund、Queensbridge Venture Partners and ZAD Investment Company、Jonathan Teo、Bill Tai

项目	类型	国家	时间	资金	融资类型	情况
BitGo	底层架构	美国	2014/09/04	N/A	N/A	BitFury Capital
			2014/06/16	1200	A 轮	Redpoint Ventures、Bitcoin Opportunity Corporation、Radar Partners、Liberty City Ventures、Crypto Currency Partners、A-Grade Investments、Jeffrey S. Skoll、Bill Lee、Founders Fund、Eric Hahn、Bridgescale Partners
			2013/03/01	200	种子轮	Bridgescale Partners、Eric Hahn、Jeff Skoll、Bill Lee、Others 未知
BitGold	数字资产	加拿大	2014/07/14	100	种子轮	Massimo Agostinelli
			2014/12/05	80	种子轮	未知
			2014/12/25	350	A 轮	PowerOne Capital、Soros Brothers Investments、Sandstorm Gold、Port Vesta Holdings
Bitinstant	支付汇款	美国	2012/10/31	150	A 轮	Winklevoss Capital, David Azar
BitKan	新闻资讯	中国	2016/04/12	160	A 轮	Bitmain Technology
BitLending Club	P2P 借贷	美国	2014/10/24	25	种子轮	LAUNCHub

Bitnet	支付 汇款	美国	2014/10/20	1450	A 轮	Highland Capital Partners、Rakuten、James Pallotta、Stuart Peterson、Bill McKiernan、Stephens Investment Management、Bitcoin Opportunity Fund、Commerce Ventures、Webb Investment Network、Buchanan Investment
			2014/01/01	N/A	种子轮	Commerce Ventures

项目	类型	国家	时间	资金	融资类型	情况
BitPagos	支付 汇款	美国	2014/06/17	60	种子轮	Pantera Capital、Boost Bitcoin Fund、8capita、South Ventures、NXTP Labs、Tim Draper、Barry Silbert、Individual Investors
			2013/09/01	3	种子轮	NXTP Labs
BitPay	支付 汇款	美国	2014/05/13	3000	A 轮	Index Ventures、AME Cloud Ventures、Felicis Ventures、Founders Fund、Horizons Ventures、RRE Ventures、Sir Richard Branson、TTV Capital、Jerry Yang、Richard Branson
			2013/05/16	200	种子轮	A-Grade Investments、Founders Fund、Heisenberg Capital
			2013/01/07	51	种子轮	Individual Investors: Shakil Khan、Barry Silbert、Roger Ver、Ashton Kutcher、Matt Mullenweg、Ben Davenport、Trace Mayer、Jimmy Furland
BitPesa	支付 汇款	肯尼亚	2015/02/09	110	A 轮	对冲基金 Pantera Capital 领投，其他参与者包括风险投资公司 Bitcoin Opportunity Corp、Crypto Currency Partners、Future/Perfect Ventures 以及 Stephens Investment Management

BitShares	交易平台	全球	2014/07/20	369	众筹	5904 个 BTC
BitSim	全产业	中国	2014/02/04	50	种子轮	Seedcoin, Individual Investors
Bitstamp	交易平台	英国	2013/10/31	1000	A 轮	Pantera Capital Management

项目	类型	国家	时间	资金	融资类型	情况
Bitt	交易平台	巴巴多斯	2016/03/31	1600	A 轮	Overstock
			2015/03/30	150	种子轮	Avatar Capital
Bitwage	工资支付		2015/11/20	76	种子轮	Cloud Money Ventures、Saeed Amidi、法国电信集团 Orange、Draper Associates、Bitcoin Capital fund 等
Bitwala	支付汇款	荷兰	2016/04/04	91	种子轮	KfW Banking Group, Digital Currency Group
BitX	交易平台	新加坡	2014/08/19	82	种子轮	Naspers 集团领投, Digital Currency Group 参投
			2015/07/21	400	A 轮	Digital Currency Group, Carol Realini
Blockchain.info	钱包服务	英国	2014/10/07	3050	A 轮	Lightspeed Ventures、Wicklow Capital、Mosaic Ventures、Prudence Holdings、Future Perfect Ventures、Rafael Corrales、Amit Jhavar、Nat Brown、Individual Investors

BlockCypher	底层架构	美国	2015/01/14	310	种子轮	Tim Draper, AME Cloud Ventures, Boost VC, 500 Startups, Crypto Currency Partners, New Enterprise Associates (NEA), Nasir Jones, Jesse Draper, Shawn Byers, Fenox Venture Capital, Streamlined Ventures, Upside Partnership, Foundation Capital
-------------	------	----	------------	-----	-----	---

项目	类型	国家	时间	资金	融资类型	情况
Blockscore	身份认证	美国	202014/6/1	3		Lightspeed Venture Partners
			2014/06/26	200	天使轮	Battery Ventures、Lightspeed Venture Partners、Boost VC、New Atlantic Ventures、Khosla Ventures、Y Combinator

Blockstream	技术服务	美国	2014/11/18	2100	天使轮	领投人分别是 LinkedIn 联合创始人兼 Airbnb 董事会成员 Reid Hoffman、Khosla Ventures（之前投资了 Chain.com）、加拿大种子基金 Real Ventures，其他投资公司也促成了这一轮融资，包括 Crypto Currency Partners、谷歌董事长埃里克·施密特的 Innovation Endeavors、Future/Perfect Ventures、Mosaic Ventures、Ribbit Capital 以及雅虎联合创始人杰里杨的 AME 云创投
			2016/02/04	5500	A 轮	领投方分别是安盛战略风险投资公司（AXA Strategic Ventures，法国跨国保险公司安盛集团的风险投资部门）、Digital Garage（由伊藤穰一联合创立的东京在线支付公司）以及香港风险投资公司 Horizons Ventures，其他参投方还包括 AME 云创投、区块链资本（Blockchain Capital）以及未来/完美风投（Future/Perfect Ventures）
BlockTrail	底层架构	荷兰	2014/08/18	65	种子轮	Lev Leviev

项目	类型	国家	时间	资金	融资类型	情况
Bonafide (Bonifide.io)	数据分析	美国	2015/02/02	85	种子轮	Quest Venture Partners, Crypto Currency Partners, AngelList Bitcoin Syndicate
			2014/10/01	N/A	种子轮	Quest Venture Partners
			2014/04/21	10	种子轮	500 Startups
BTC China (Shanghai Satuxi Network)	交易平台	中国	2013/11/18	500	A 轮	Lightspeed China Partners,
BTC. sx	交易平台	新加坡	2014/04/01	30	种子轮	Seedcoin, Joe Lee
BTCS	挖矿	美国	2015/12/22	145	N/A	Cavalry Fund I LP
			2015/04/27	230	N/A	未知
			2015/01/01	50	N/A	未知
Buttercoin	底层架构	美国	2013/09/01	125	A 轮	Alexis Ohanian、Centralway、FLOODGATE、Google Ventures、Initialized Capital、Rothenberg Ventures、Y Combinator
Case	硬件钱包	美国	2015/06/18	150	种子轮	Future/Perfect Ventures 领投, RRE Ventures、Third Kind Venture Capital、Rochester Institute of Technology
			2015/09/11	100	种子轮	Future/Perfect Ventures 领投

项目	类型	国家	时间	资金	融资类型	情况
Chain	技术服务	美国	2014/01/01	420	天使轮	Betaworks、RRE Ventures, Thrive Capital 和 SV Angel
			2014/08/21	950	A 轮	由 Khosla Ventures 领衔, 由计算机巨头 Sun Microsystems 公司的联合创始人 Vinod Khosla 发起, 投资者包括 Kevin Ryan、Barry Silbert、Scott Banister, Homebrew、500 初创公司以及 Pantera Capital
			2015/09/10	3000	B 轮	Visa 公司、纳斯达克、花旗风投、RRE Ventures、第一资本金融公司、Fiserv 公司、Orange SA 等金融巨头
Chainalysis	数据分析	美国	2016/02/22	160	天使轮	Point Nine Capital、TechStars、Digital Currency Group (数字货币集团)、FundersClub、Converge Venture Partners
Challenger Deep	底层架构	英国	2015/07/23	186	种子轮	Pascal Gauthier
ChangeTip	支付汇款	美国	2014/12/02	350	A 轮	Pantera Capital、500 Startups、Boldstart Ventures、CryptoCurrency Partners、Idealab
			2014/05/05	75	种子轮	CryptoCurrency Partners
			2014/04/04	N/A	种子轮	BOLDstart Ventures

Chronicled	底层架构	美国	16/03/09	342	种子轮	Mandra Capital、Pantera Capital、Colbeck Capital Management
------------	------	----	----------	-----	-----	---

项目	类型	国家	时间	资金	融资类型	情况
Ciphrex	钱包服务	美国	2015/01/15	50	A 轮	未知
			2014/10/07	30	N/A	未知
Circle	支付汇款	美国	2013/10/31	900	A 轮	Accel Partners, General Catalyst Partners
			2014/05/26	1700	B 轮	Breyer Capital、General Catalyst Partners、Oak Investment Partners 以及 Accel Partners
			2015/04/30	5000	C 轮	高盛以及 IDG 资本（中国）领投，Breyer Capital、General Catalyst Partners、Oak Investment Partners 以及 Accel Partners 跟投
Civic	身份认证	美国	2016/01/29	275	天使轮	领投方为 Social Leverage 风投公司，其他参与方包括 Founder Collective、Pantera Capital、Blockchain Capital 以及 Digital Currency Group
Coinalytix	数据分析	美国	2014/04/21	10	种子轮	500 Startups
			2015/09/11	110	种子轮	The Hive 领投、SeanPercival、Dave McClure、500Fintech, 500 Startups
Coinapult	钱包服务	巴拿马	2014/09/30	78	种子轮	Bitcoin Opportunity Corp、Roger Ver、FirstMark Capital、Erik Voorhees、Ira Miller

项目	类型	国家	时间	资金	融资类型	情况
Coinbase	全产业	美国	2015/01/20	7500	C 轮	领投方包括 DFJ Growth、Andreessen Horowitz、Union Square Ventures，以及 Ribbit Capital；此外还有纽约证券交易平台（NYSE）、财富 500 强金融服务集团 USAA、西班牙外换银行 BBVA 以及日本电信巨头 DoCoMo 也参与了融资
			2013/12/12	2500	B 轮	Andreessen Horowitz, Ribbit Capital, Union Square Ventures, QueensBridge Venture Partners, Anthony Saleh, Nasir “Nas” Jones
			2013/04/26	611	A 轮	Ribbit Capital、Union Square Ventures、Red Swan Ventures、SV Angel, Interplay Ventures、FundersClub
			2012/09/01	60	种子轮	Alexis Ohanian、Y Combinator、Greg Kidd, Garry Tan、Funders-Club
coinfirma	挖矿	美国	2013/12/31	50	种子轮	未知 Venture Investor(s)
Coinfloor	交易平台	英国	2014/06/06	20	N/A	Passion Capital、Taavet Hinrikus、Adam Knight
			2013/09/08	10	种子轮	Passion Capital、Taavet Hinrikus、Individual Investors

Coinify *	全产业	丹麦	2014/09/25	34	种子轮	SEED Capital
Coinigy	交易平台	美国	2015/03/19	10	种子轮	未知

项目	类型	国家	时间	资金	融资类型	情况
CoinJar Pty	钱包服务	澳洲	2013/12/02	50	A 轮	Blackbird Ventures, Individual Investors
			2013/05/01	2	种子轮	AngelCube
CoinOutlet	ATM 交易平台	美国	2015/01/01	10	种子轮	BTCS
			2014/11/01	5	种子轮	BitcoinShop
Coinplug	支付汇款	韩国	2013/11/25	40	种子轮	Silverblue
			2014/04/03	40	种子轮	Draper Fisher Jurvetson Partners、Key Initiatives Technical Entrepreneur、Individual Investors
			2014/10/08	250	A 轮	Mirae Asset Venture Investment、Bokwang Investment Corp、Capstone Partners、DSC Investment、Tim Draper
			2015/10/03	500	B 轮	SBI Investment
CoinPlus	支付汇款	卢森堡	2014/09/18	22	种子轮	未知
Coinsetter	交易平台	美国	2014/10/16	140	B 轮	Unknown
			2014/02/18	50	A 轮	Crypto Currency Partners
CoinSimple	支付汇款	中国	2014/03/07	18	种子轮	Seedcoin, Individual Investors

Colu	数字资产	以色列	2015/01/27	250	A 轮	Aleph Capital、Spark Capital、BoxGroup 以及 Bitcoin Opportunity Fund
Counterparty	底层架构	全球	2014/02/03	172	众筹	2126 个 BTC

项目	类型	国家	时间	资金	融资类型	情况
Cryex	交易平台	瑞典	2015/05/07	1000	A 轮	White Star Capital, Northzone Ventures
Cryptopay	支付汇款	英国	2014/02/04	8	种子轮	Seedcoin
Custos Media Technologies	数据认证	南非	2016/04/08	27	种子轮	Digital Currency Group、Innovus Technology Transfer、未知 angel investor
Dacplay	智能合约	全球	2015/02/23	57	众筹	2397 个 BTC
Devign Lab	全产业	韩国	2014/10/09	20	种子轮	K Cube Ventures
DigiByte	支付汇款	美国	2014/12/02	25	种子轮	未知
Digital Asset Holdings	技术服务	美国	2016/02/02	6000	A 轮	高盛、IBM、荷兰银行、埃森哲、澳洲证券交易平台、法国巴黎银行、Broadridge 的金融解决方案、花旗银行、CME Ventures、德意志交易平台集团、ICAP、桑坦德风投、证券托管清算公司 (DTCC)、PNC 金融服务集团
Digital Currencies FinTech	新闻资讯	美国	2013/08/19	125	A 轮	Centralway AG、Floodgate、Google Ventures、Individual Investors、Initialized Capital、Y Combinator

DigixDao	数字资产	全球	2016/03/31	550	众筹	13290 个 BTC
Dogtipbot	支付汇款	美国	2014/11/05	45	种子轮	Blackbird Ventures、Scott and Cyan Banister、Individual Investors

项目	类型	国家	时间	资金	融资类型	情况
Elliptic	钱包服务	英国	2016/03/21	500	A 轮	Paladin Capital Group、Santander InnoVentures、KRW Schindler、Digital Currency Group; Octopus Ventures
			2014/07/16	200	种子轮	Octopus Investments
			2014/02/10	N/A	种子轮	Seedcamp
Ethcore	底层架构	英国	2016/04/22	75	Pre-种子轮	Blockchain Capital, Fenbushi Capital
Ethereum	底层架构	全球	2014/08/01	1820	众筹	
Exchange of the Americas (meXBT)	交易平台	墨西哥	2014/03/18	34	种子轮	Seedcoin, Individual Investors
			2014/01/15	15	种子轮	Seedcoin, Individual Investors
Expresscoin	交易平台	美国	2014/07/01	15	种子轮	BTCS
			2014/03/01	N/A	种子轮	Crypto Currency Partners, Demarest
			2014/03/01	N/A	种子轮	Crypto Currency Partners
Factom	数据认证	美国	2015/05/01	120	众筹	
			2015/10/15	180	种子轮	Kuala Innovations

Filament	物联网	美国	2014/08/19	100	种子轮	VTF Capital, Resonant Venture Partners
			2015/08/18	500	A 轮	Bullpen Capital、Crosslink Capital、Haystack、Techstars、Verizon、Digital Currency Group、Samsung Ventures、Working Lab Capital

项目	类型	国家	时间	资金	融资类型	情况
Gem	技术服务	美国	2015/01/21	10	天使轮	Amplify. LA
			2014/05/09	190	种子轮	Mesa Ventures、Idealab、James Joaquin、Brock Pierce 的投资公司、Crypto Currency Partners 的投资
			2015/02/15	132.5	种子轮	KEC Ventures 领投，其他跟投方包括 First Round Capital、RRE Ventures（参与了 21 Inc 和 Abra 的投资）、Facebook 的早期投资人 Robert Wolfson 等
			2016/01/06	710	A 轮	领投方为 Pelion 风险投资合伙公司，跟投方包括 KEC 风险投资公司、Blockchain Capital、Digital Currency Group、RRE Ventures、Tamarisk Global、Drummond Road Capital、Tekton Ventures、Amplify. LA、Danmar Capital 以及天使投资人 James Joaquin
GetGems	社交通信	以色列	2015/01/05	40	种子轮	Magma VC
			2014/12/01	60	种子轮	未知
			2015/02/06	56.8	众筹	2633 个 BTC

Gliph	社 交 通 信	美国	2014/01/31	3	种子轮	Semil Shah
			2013/12/18	13	种子轮	Pantera Capital
			2013/09/19	20	种子轮	Boost Fund、Portland Seed Fund、 Rogue Venture Partners、Tim Draper、Individual Investors
			2013/05/18	2	种子轮	N/A
			2012/01/03	3	种子轮	Portland Seed Fund

项目	类型	国家	时间	资金	融资类型	情况
GoCoin	支付汇款	新加坡	2014/03/26	150	A 轮	BTCS、Crypto Currency Partners、Owen Van Natta、Demarest、Individual Investors
			2013/11/07	55	种子轮	BitAngels、Demarest Ventures、Individual Investors、Ruvento Ventures、Crypto Currency Partners、Gary Stiffelman、Mikael Pawlo、Andrew Frame、Owen Van Natta、David Neuman、Ronnie Wee、Honathan Congdon、Prolific Venture Capital
GogoCoin	钱包服务	美国	2014/04/21	10	种子轮	500 Startups
			2013/10/09	11	种子轮	500 Startups, Draem Ventures
			2013/10/01	1	种子轮	Draem Ventures
HashPlex	挖矿	美国	2014/06/12	40	种子轮	Barry Silbert、Jason Prado、Individual Investors
HashRabbit	挖矿安全	美国	2015/02/04	50	种子轮	Draper Associates, VegasTechFund
			2014/10/01	20	N/A	VegasTechFund
Hedgy	智能合约	美国	2015/04/30	120	种子轮	Draper Fisher Jurvetson、Tim Draper、Marc Benioff (Salesforce 的 CEO)、Sand Hill Ventures 等

Hive	钱包服务	中国	2014/03/26	19	种子轮	Roger Ver, Seedcoin
Huobi	交易平台	中国	2014/05/27	1000	A 轮	Sequoia Capital China

项目	类型	国家	时间	资金	融资类型	情况
iBit	交易平台	美国	2015/05/07	2500	A 轮	RRE Ventures、Liberty City Ventures、投资人 Jay W Jordan II. 以及 Raptor Capital 管理公司董事长 James Pallotta
			2013/11/11	325	A 轮	Canaan Partners、Individual Investors、Liberty City Ventures、RRE Ventures、Jay W. Jordan II、Ben Davenport
Keza	交易平台	美国	2016/03/02	36	Pre-种子轮	Jason Calacanis, Digital Currency Group
KnCMiner	挖矿	瑞典	2015/02/03	1500	B 轮	Accel Partners、GP Bullhound、Creandum, Martin Wattin
			2014/09/04	1400	A 轮	Creandum
Koinify	数字资产	美国	2014/09/17	100	A 轮	IDG Capital Partners、zPark Ventures、Danhua Capital、Brock Pierce、Individual Investors
			2014/03/25	45	种子轮	Zhenfund (Sequoia China Angel)、Ceyuan Ventures、Crypto Currency Partners

Korbit	全产业	韩国	2014/08/25	300	A 轮	Pantera Capital、BAM Ventures、Bitcoin Opportunity Corp、Tim Draper、Pietro Dova、Strong Ventures、Softbank Ventures Korea
			2014/01/20	40	种子轮	Strong Ventures、Bitcoin Opportunity Fund、Tim Draper、David Lee、Naval Ravikant、Michael Yang、Jay H. Eum、Pietro Dova

项目	类型	国家	时间	资金	融资类型	情况
Kraken	交易平台	美国	2013/12/31	500	A 轮	Hummingbird Ventures 领投, Digital Currency Group、Blockchain Capital, 以及 Roger Ver 等 12 位个人投资者
Ledger	硬件钱包	法国	2015/02/19	150	种子轮	法国风投基金 XAnge Private Equity 领投, 其他参与者还有 Hi-Pay (高新传媒集团)、NetAtmo 首席执行官 Fred Potter、Rentabiliweb 集团副总裁 Thibaut Faurès Fustel de Coulanges、Alain Tingaud Innovations 和 Pascal Gauthier、Criteo 的前任首席执行官以及 Challenger Deep 创始人
LibertyX	ATM 交易平台	美国	2015/01/07	40	种子轮	Project 11
Libra	技术服务	美国	2014/10/10	50	种子轮	Liberty City Ventures、James Pallotta、Ben Davenport、CrossCoin Ventures
Lisk	底层架构	全球	2016/03/21	620	众筹	15128 个 BTC
Lota	物联网	全球	2015/12/22	52.4	众筹	1191 个 BTC

Melotic	交易平台	中国	2014/10/10	118	种子轮	Ceyuan Ventures、Lightspeed China、Bitcoin Opportunity Corp、500 Startups、Marc Van Der Chijs
Metafees	交易平台	全球	2015/12/18	4.6	众筹	102 个 BTC

项目	类型	国家	时间	资金	融资类型	情况
Mirror	智能合约	美国	2014/05/07	400	种子轮	Battery Ventures、Tim Draper 以及 AOL 首席执行官 Steve Case
Mirror Labs	智能合约	美国	2015/06/03	880	A 轮	Route 66 Ventures 领投，其他跟投方包括 Battery Ventures、Crosslink Capital、RRE Ventures 以及 Tim Draper
Monetsu	支付汇款	美国	2014/04/21	10	种子轮	500 Startups
Muse	娱乐	全球	2014/12/05	53.2	众筹	1438 个 BTC
NeuCoin	支付汇款	法国	2015/02/03	125	种子轮	Patrik Stymne、Emil Michael、Henrik Kjellberg
Neuroware	钱包服务	美国	2014/04/21	10	种子轮	500 Startups
OKCoin	交易平台	中国	2014/03/16	1000	A 轮	Ceyuan、Mandra Capital、VenturesLab、PreAngel、Individual Investors
			2013/09/04	100	种子轮	Ventures Lab
Omni		全球	2013/09/01	56.8	众筹	4740 个 BTC
OneName	身份认证	美国	2014/11/16	150	种子轮	Union Square Ventures、Naval Ravikant、SV Angel
			2014/07/16	12	种子轮	Y Combinator

OpenBazaar	电子商务	未知	2015/06/11	100	种子轮	Andreessen Horowitz、Union Square Ventures、William Mougayar、天使投资人 William Mougayar
------------	------	----	------------	-----	-----	---

项目	类型	国家	时间	资金	融资类型	情况
Orb	钱包服务	日本	2015/10/06	230	种子轮	Adways Inc、Ceres、Monex Ventures、SBI Investment
Paymium	支付汇款	法国	2011/12/21	40	种子轮	Galitt
			2015/09/03	112	天使轮	Newfund 以及 Kima Ventures 风投公司
PayStand	支付汇款	美国	2014/04/02	100	种子轮	Cervin Ventures、Serra Ventures、Central Coast Angels、TiE Launch-Pad
Payward, Inc. (Kraken)	交易平台	美国	2014/03/25	500	A 轮	Hummingbird Ventures、Trace Mayer、Bitcoin Opportunity Fund.
			2013/12/20	150	种子轮	Crypto Currency Partners
PeerNova	底层架构	美国	2015/03/31	500	A 轮	OverStock
PeerNova	挖矿	美国	2014/12/17	860	A 轮	Mosaik Partners 领投, 前 AOL 首席执行官 Steve Case、Crypto Currency Partners、Atiq Raza, Ashar Aziz 也参与了融资
Pey	底层架构	德国	2015/09/17	34	种子轮	Marc Junker, Frank Biedka, Hartmut A Borchers, Jürgen Pleiteit, Olav Vier genannt Strawe, Tobias Jankowiak

Purse	钱包服务	美国	2014/11/27	27.5	种子轮	FundersClub, Roger Ver
Purse	钱包服务	美国	2015/12/07	100	种子轮	Digital Currency Group、Bitcoin by Flight. vc、TA Ventures、Roger Ver

项目	类型	国家	时间	资金	融资类型	情况
Reveal	社交通信	美国	2015/06/16	150	种子轮	Mike Hirshland、Boost VC、Digital Currency Group、the Stanford StartX Fund、Barry Silbert
Ribbit. me	工资支付	美国	2016/02/26	150	种子轮	Hayaat Group
Ripple Labs	底层架构	美国	2013/04/11	未知	种子轮	Andreessen Horowitz、Lightspeed Venture Partners、FF Angel
			2013/05/14	未知	种子轮	GV, IDG Ventures
			2013/11/12	350	种子轮	IDG Ventures
Ripple Labs	底层架构	美国	2015/05/18	3200	A 轮	Santander InnoVentures、IDG Capital Partners、CME Group、Seagate Technology、AME Cloud Ventures、ChinaRock Capital Management、China Growth Capital、威克洛资本、Bitcoin Opportunity 公司、核心创新资本、美国 Route 66 Ventures、RRE Ventures、Vast Ventures 以及 Venture 51

Rootstock	智能合约	阿根廷	2016/01/15	10	种子轮	伦敦区块链投资公司 Coinsilium
			2016/03/21	100	种子轮	Bitmain Technology、Coinsilium、Digital Currency Group
Safe Cash	数字资产	美国	2015/09/30	120	种子轮	InfoSpace 创始人 Naveen Jain
Safe Exchange	智能合约	全球	2016/01/06	4.8	众筹	112 个 BTC

项目	类型	国家	时间	资金	融资类型	情况
Safe Network	底层架构	全球	2014/05/23	644	众筹	12200 个 BTC
Safello	交易平台	瑞典	2014/07/10	25	种子轮	Bitcoin Opportunity Corp
			2014/02/17	60	种子轮	Roger Ver、Nicolas Cary、Eric Voorhees、Individual Investors
Satoshi Citadel Industries Inc.	全产业	菲律宾	2015/05/06	10	种子轮	Joe Maristela
SatoshiPay	支付汇款	英国	2016/09/22	20	种子轮	Kuala Innovations
			2016/01/25	39	种子轮	Coinsilium, FastForward Innovations
Scorechain	合规方案	卢森堡	2015/10/13	57	天使轮	未知
			2015/10/12	57	种子轮	未知
ShapeShift	交易平台	瑞士	2015/03/10	52.5	种子轮	Barry Silbert, Roger Ver
			2015/09/09	160	A 轮	领投方为 Digital Currency Group、Roger Ver、Bitfinex, 跟投方包括比特币基金会执行主任 Bruce Fenton、Transform PR 公司创始人兼首席执行官 Michael Terpin 以及教育性电子商务平台 eProf 创始人 Trevor Koverko

ShoCard	底层架构	美国	2015/07/17	150	种子轮	AME Cloud Ventures、Digital Currency Group、Enspire Capital、Morado Venture Partners
Simplex	支付汇款	以色列	2016/02/04	700	A 轮	Bitmain、Cumberland Mining、FundersClub、未知 angel investors

项目	类型	国家	时间	资金	融资类型	情况
SNAPCARD	支付汇款	美国	2014/10/06	150	种子轮	Tim Draper、Crypto Currency Partners、Insikt Ventures、Great Oaks Venture Capital、Boost VC、Seed-Invest、Silicon Valley Angels、Fortress Investment Group、Individual Investors
			2013/12/01	6	N/A	Ioannis Giannaros、Michael Dunworth、Boost VC
SolidX	交易平台	美国	2014/10/07	300	A 轮	Liberty City Ventures、James Pallotta、Red Sea Ventures and Red Swan Ventures
Spondoolies-Tech	挖矿	以色列	2014/10/24	500	B 轮	Agile Wings、BRM Group、Genesis Partners、Olivier Janssens、E-den Shochat、Individual Investors
			2014/02/01	150	Bridge	Genesis Partners、BRM、Individual Investors
			2013/08/01	400	A 轮	Genesis Partners、BRM、Individual Investors
Stampery	数据认证	美国	2015/11/18	60	天使轮	Draper & Associates、Blockchain Capital、天使投资人 Di-Ann Eisnor
Storj	存储	全球	2014/08/19	42.7	众筹	910 个 BTC

Stratumn	底层 框架	法国	2016/03/30	70	种子轮	Otium Venture, Eric Larchevêque
Streami	支付 汇款	韩国	2015/12/25	200	天使轮	新韩银行领投，其他投资方还包括支付公司 ICB、风险投资公司 Bluepoint Partners，以及一群天使投资人

项目	类型	国家	时间	资金	融资类型	情况
SuperNET		全球	2014/09/24	243	众筹	5737 个 BTC
SurBTC	交易平台	智利	2016/02/04	30	种子轮	Digital Currency Group、Sausalito Ventures、智利律师事务所 Barros & Errazuriz 的创始人
Swarm	数字资产	美国	2014/10/10	12	种子轮	Techstars
			2014/07/21	78.9	众筹	1270 个 BTC
Symbiont	智能证券	美国	2015/06/09	125	种子轮	投资者包括 Citadel Derivatives Group 联席首席执行官 Matt Andresen, 以及前纽约证券交易平台首席执行官 Duncan Niederauer
TabTrader	交易平台	荷兰	2015/07/16	10	种子轮	IMPACT
			2015/03/20	7	种子轮	Rockstart
Tangible Cryptography (BitSimple)	交易平台	美国	2014/01/21	60	种子轮	未知
Tembusu	ATM 交易平台	新加坡	2014/03/12	24	种子轮	Individual Investors
			2015/01/29	88.7	A 轮	未知
Tibdit	汇款支付	英国	2015/07/01	19	众筹	
			16/04/22	16	种子轮	Private

TradeBlock	数据分析	美国	2014/07/16	280	种子轮	Andreessen Horowitz、Barry Silbert、Devonshire Investors、FinTech Collective、Y Combinator、Data Collective、Bitcoin Opportunity Corp.、Chris Fisher、Hard Yaka
TradeHill	交易平台	美国	2013/03/01	40	种子轮	Individual Investors

项目	类型	国家	时间	资金	融资类型	情况
Trustatom	身份认证	加拿大	2015/01/20	10	种子轮	Brian Cartmell, Vinny Lingham
Unocoin	全产业	印度	2014/08/11	25	种子轮	Bitcoin Opportunity Corp
Uphlod (Bitreserve)	钱包服务	美国	2014/12/30	960	B 轮	157 位投资人, 最大单笔投资达到了 776.9
			2014/03/31	500	A 轮	未知
Vaurum	交易平台	美国	2014/05/07	400	种子轮	Battery Ventures、Tim Draper、Steve Case、QueensBridge Venture Partners
			2013/09/01	200	A 轮	Boost Fund
Vogogo	支付汇款	加拿大	2015/06/24	1250	B 轮	Beacon Securities、Clarus Securities、Salmon Partners
			2014/08/05	850	A 轮	Beacon Securities、Clarus Securities、Salmon Partners、Canaccord Genuity Corp、Cormark Securities Inc.
Volabit	交易平台	墨西哥	2014/07/23	75	种子轮	Tim Draper、Boost VC、Bitcoin Opportunity Fund, individual investors

Xapo	钱包服务	美国	2014/07/08	2000	A 轮	Index Ventures、Greylock Partners、Emergence Capital Partners、Yuri Milner、Max Levchin、Jerry Yang、Winklevoss Capital、David Marcus、Crypto Currency Partners
			2014/03/13	2000	A 轮	Benchmark、Fortress Investment Group、Ribbit Capital、Slow Ventures

项目	类型	国家	时间	资金	融资类型	情况
ZapChain	社交网络	美国	2015/11/07	35		德丰杰（DFJ）合伙人 Tim Draper、Boost VC 创始人兼首席执行官 Adam Draper 以及 Boost 比特币基金
Zebpay	钱包服务	印度	2015/01/05	100	A 轮	纺织行业资深人士 Amit Jindal、Claris 生命科学副主任 Arjun Handa、工程师兼开发人员 Nagesh Chaudhary
Ziftr	电子商务	美国	2015/02/03	85	种子轮	10x Venture Partners

第八章 各国对区块链的法律监管情况

一、各国政府或地区如何监管数字货币与区块链

关于比特币，全球各辖区的法规变得越来越清晰。在美国有一些立法或监管进行了更新，判例法也进一步规定了比特币是如何定义的。在美国以外的地区，众多的金融监管机构都在权衡应该如何接受比特币和持有人应该如何纳税这些情况。

（一）美国

1. 证券交易委员会指控比特币的庞氏骗局

美国证券交易委员会控告一名得克萨斯州男子通过比特币进行庞氏骗局，并称为“比特币储蓄和信托”（Bitcoin Savings and Trust, BTCST），以及销售未经注册的金融证券欺诈，这是SEC在2013年第三季度在美国实施的最明确的行动之一。2011年和2012年，BTCST通过承诺过高的利率和模糊描述交易方式获得了700000个BTC的投资。

尽管这个案件显示SEC对比特币计价的证券欺诈罪起诉的意愿，更重要的意义在于法官针对被告人辩解的回应。BTCST的运营商特雷顿·沙弗尔（Tredon Shavers）辩称，因为其所有交易是基于比特币，实际上没有任何金钱经手和投资BTCST的不是真正证券。此案的主审法官宣布，“比特币可以兑换为传统货币……因此，比特币是货币或货币的一种形式”。

2.比特币基金会与监管机构、立法者

比特币基金会作为规范、保护和促进使用比特币的非营利组织，在2013年8月的两天时间里，会见了监管机构和立法者，并回答了他们关心的问题。在有12个联邦机构参与的第一天会议上，议题主要侧重于国土安全部、司法部、联邦调查局、国税局、特勤局和金融犯罪执法网络（FinCEN）等监管机构所关注的方面，比特币可以用于非法目的，同时也有潜力能增加金融体系的效率。而在第二天的会议上，包括参议院和众议院在内的五个立法机构的国会工作人员，与基金会围绕金融隐私进行了讨论。鉴于有关比特币区块链的公开特性，立法者的关注点都集中在如何确保充分保护消费者。

3.22个比特币公司被传唤

2013年8月，纽约州金融服务部（DFS）传唤了与比特币行业相关的22家公司。这些公司包括了从交易所和支付处理公司到挖矿硬件厂商和对比特币进行投资的风投公司。大多数的公司都位于纽约州之外。

在纽约DFS的管理者解释了之所以发传票传唤一些公司，是因为订单处理延迟造成了客户投诉，也说明了进一步了解该行业是一个更好的选择。许多比特币行业内的公司会自愿让监管者对其进行研究，花费私人资源来起草法律以回应非正式的指控，这比用国家资源来调查行业行为要更好。迄今为止，没有因传票而产生的诉讼被提交给州政府。

4.美参院听证会“承认”比特币合法性

2013年11月18日，在美国参议院国土安全及政府事务委员会召开有关比特币的听证会上，多名出席的美国政府官员对外传递出一个信息——比特币不是非法货币，能够给金融系统带来好处，尽管其也存在被错误使用的案例。这场有史以来首次就数字货币举行的美国国会听证会，总结了比特币的优势和弊端。以往官员们都是强调比特币在洗钱及

其他非法活动中所扮演的角色，但这一次却表示，比特币是一项“合法”的金融服务，这是美国政府首次公开承认比特币的合法性，同时也意味着这种数字货币朝主流方向迈进了一大步，这给比特币交易者提振了不少信心。

美国官员的积极表态助推比特币价格再创历史新高。11月19日，比特币价格在Mt.GOX交易平台最高攀升至900美元，在比特币中国交易平台（BTC China）最高攀升至6989元人民币。而2012年年底比特币的价格还处于13美元左右，2013年上半年曾出现过266美元的高位，但之后又再次震荡，会议的前一周（11月11日），比特币的交易价格在320美元左右。

5.伯南克致信“唱多”

在上述名为“数字货币潜在的威胁、风险和前景”的美参议院听证会上，出席人员不仅包括美国司法部刑事部门的代理助理部长密斯里·拉曼（Mythili Raman）、美国财政部金融犯罪执法局局长珍妮弗·夏斯基·卡尔韦里（Jennifer Shasky Calvery）、美国特勤局特工爱德华·朗利（Edward Lowery），还有从事比特币业务的人员和相关学者。不少从事比特币业务的人发现在美国很难说服传统银行与之交易，但比特币的爱好者们坚信，国会对于比特币“风险”和“前景”较为平衡的讨论有利于缓和这种气氛。

值得注意的是，美国联邦储备委员会主席伯南克没有出席听证会，但他在致参议院的信中，援引美联储前副主席艾伦·布林德（Alan Blinder）在1995年时的表态称，美联储一直认为在数字货币带来洗钱和其他风险之时，也可能带来长期效益，特别是如果这种创新催生出一个更快、更安全、更高效的支付系统。伯南克的话使得比特币的狂热者们注意到了比特币价值所在，即作为目前全球资金转移体系的廉价替代品。不过，伯南克也在信中指出，美联储并没有太多权限来监管数字货

币，“尽管美联储通常在监控数字货币的发展，以及其他支付方式的创新，但这并不代表我们有权力直接监督或监管这些新的创新”。

6.“积极制定”有关税则

无论是伯南克还是其他美国官员，几乎都将比特币与创新相挂钩，认为不应该扼杀创新。

在认定数字货币存在可取之处以外，听证会的参与人员还表示，目前数字货币依然存在问题没有解决答案。参议院国土安全及政府事务委员会主席托马斯·卡珀（Thomas Carper）举例称，数字货币到底是什么，应该如何对待以及其未来到底能够做什么，这些基础问题仍需要解决，并表示国会和联邦机构必须持续关注并参与其中，研究出适合、有效和明智的决策，比特币价格高涨，加之这种货币在网络和实体零售商的使用量大增，都引起了华盛顿的关注。美国监管部门警告说，比特币转账业务必须遵循与现有金融机构同样的规定，包括遵守反洗钱法等。有关部门开始与其他政府机构会谈，追踪最新进展，其中一个由美国联邦调查局牵头的小组在调查与此技术有关的新型威胁。

7.美国国家税务局开始对比特币交易活动征税

2014年3月26日，美国国家税务局（IRS）发布了一项正式通知，称它们有权对比特币交易活动征税，并将其称为是一种财产，而不是一种货币。这代表来自美国政府的一个信号，标志着当局将严肃对待这一产品。

IRS在通知中明确表示，与比特币有关的交易活动的交易额若是突破了600美元，便应以产权交易的相关规定来收取税金。这包括用比特币支付购买其他商品，通过对其投资获得的收益以及通过电脑开采比特币——即“挖矿”的所得。如果公司用比特币给员工发薪水，那么应该标记在W-2收入报税表上，并且应该缴纳联邦所得税。若是从独立契约人

那里收取报酬，则需登记在1099报税表（Form 1099）上。使用数字货币支付将与其他财产支付手段一样进行必要的记录和登记。

尽管从法律角度上来说，比特币在美国不具有法定货币的地位，但它仍然是一种数字货币。IRS承认比特币和其他电子代币具有与真实货币一样的功能，但是拒绝对此下明文定义，IRS表示比特币的“公平市价”按照人们得到它的那一刻计算，但这不是一件容易的事，因为它的价格时时刻刻都在变化。IRS表示纳税者在纳税时可以按照在线交易所的价格计算。

8.数字货币公司监管框架BitLicense被发布

2015年6月4日，纽约金融服务部门（NYDFS）发布了最终版本的数字货币公司监管框架BitLicense。该版本的BitLicense在经过了近两年时间的调查以及争论后正式推出。需要注意的是，在纽约州登记处（New York State Register，纽约州政府每周颁布的规章制定指南）颁布该法案之后，该监管框架才能正式成为法律。

纽约金融服务部门主管本杰明·劳斯基（Benjamin Lawsky）阐明说，最终的法规意味着，该机构不需要为每一个企业的软件更新或者风险投资进行批准。另外，企业还可以“一站式”提交BitLicense以及货币汇兑许可证的申请。劳斯基表示，数字货币具有帮助金融服务部门驱动僵化支付系统的潜力。他们只是希望确保落实到护卫栏，在保护消费者和根除非法活动的同时，也不会扼杀创新。

在2015年2月发布的修订版BitLicense中，由数字货币社区提出的若干建议得到了纽约金融服务部门的认可，包括豁免了从事开源协议开发、小额支付，以及两年安全期阶段内的创业公司。劳斯基强调，该法案只适用于“金融中介”公司，而非软件提供商。

但是人们在对最终版本的BitLicense的评价上产生了严重的分歧：

一方极力赞扬BitLicense，称其为监管史上的里程碑；另一方则认为这一监管框架根本不够好。的确如此，即使BitLicense成功地使数字货币行业“合法化”了，但是很明显，这一行业中的参与者不仅仅认为只要规范数字货币行业就行了。换句话说，他们认为监管者不能用规范现有科学技术的方法来规范数字货币行业，因为这一行业有其特殊情况，否则就会阻碍这一行业的创新。BitLicense过于针对特定技术，这意味着比特币初创公司面临的门槛比那些传统的金融服务公司更高，所承担的费用也更高。BitLicense给仍处于初期阶段比特币生态系统强加了很多的限制，阻碍了数字货币和区块链技术的创新。因为BitLicense相关公司可能会违反隐私规则，增加数据和存储用户信息的泄露风险。

波士顿比特币创业公司Circle从纽约州监管机构那里拿到了第一张数字货币许可证BitLicense，这意味着该公司将可在纽约州持证提供数字货币服务。

9. 比特币被定义为大宗商品

2015年9月，美国商品期货交易委员会（CFTC）发布文件，首次把比特币和其他数字货币合理定义为大宗商品，与原油或小麦的归类一样。这意味着比特币期货和期权要符合CFTC的规定并接受监管，交易行为需要遵守所有大宗商品衍生品市场规则。如果发生期货市场操纵等不正当行为，CFTC将能够对此行为进行惩罚。美国商品期货交易委员会解释说，在该文件中，CFTC首次把比特币和其他数字货币合理地定义为大宗商品。纽约法学院教授休曼·萨达伯（Houman Shadab）称，这个文件打消了把数字货币归为证券的想法，否则这份文件就将由证交会提出。

长期以来，投资者都在讨论比特币能否被定义为大宗商品，CFTC也同样在考虑这种数字货币是否归自己监管。2014年，CFTC主席就告诉美国参议院委员会监管比特币衍生品。

如果想运营一个比特币衍生品交易平台，那么企业需要进行登记，就像CME集团（芝加哥商品交易所）做的那样。美国监管机构命令Coinflip和其首席执行官弗朗西斯科·莱尔顿（Francisco Riordan）关闭未登记的比特币期权交易平台Derivabit，原因是它们不符合商品交易法案和其他规定。这家交易平台提供“管理比特币波动的金融衍生品”。CFTC执行主管伊坦·吉尔曼（Aitan Goelman）还称，虽然比特币和其他数字货币交易相比较为活跃，但是创新不是借口，它们同样也要遵守所有大宗商品衍生品市场的规则。

同样是在9月，CFTC对名为TerraExchange的一家比特币掉期交易平台进行处罚。CFTC指控该平台为非法洗钱提供便利，并且通过新闻稿和政府赞助的公开会议误导监管者。TerraExchange设计了这样一种比特币掉期产品销售过程：价格根据2014年10月的比特币币值制定。只有两个买家获准从事该产品的交易，他们均购买相同规模和数量的掉期产品。CFTC认为，这相当于通过非法洗钱交易抵消了彼此的头寸。TerraExchange之后参加了CFTC顾问委员会会议，宣称这一交易是市场正常的买卖兴趣所致，并未经过事先安排。

10.北卡罗来纳州豁免比特币

2015年12月，美国北卡罗来纳州特别指出，监管条例会豁免比特币和区块链企业，旨在根据行业支持者要求来避免和美国其他州发生冲突。

根据已经大幅度更新的货币传输常见问答页面，北卡罗来纳州的银行专管办公室（the North Carolina Office of the Commissioner of Banks, NCCOB）在该州的货币传输法案（Money Transmitters Act, MTA）中特别免去了数字货币挖矿者，非金融类的区块链服务、多签名和非保管类的钱包服务提供者。

11.奥巴马政府参与区块链联盟

2015年10月，奥巴马政府已经和私人公司结成伙伴关系，目标是针对数字货币比特币来培训执法机构，对抗将数字货币用于非法用途。这个被称为“区块链联盟”的伙伴关系，其目标包括教育调查员应该使用数字货币及其在技术上如何运作，并且增强数字货币的信誉。

这个联盟的名字来源于该技术名字“区块链”，这是指比特币所应用在公开账本上的一种技术。支持者认为，比特币用一种去中心化的方式来为用户在交易时提供一定程度的隐私，这是一种已经获得监管部门和企业之间合法性，且快速便捷的支付系统。纽约州监管机构也批准了他们第一个获得经营数字货币许可证的企业，而在线零售商Overstock.com于2015年已经在他们位于盐湖城的总部安装了第一台比特币ATM机。

但比特币的声誉依旧被犯罪行为所困扰，它经常被用于庞氏骗局，并且是互联网最大的地下黑市“丝绸之路”的主要应用，丝绸之路的创始人在也已经被判处终身监禁。

杰里·布里托（Jerry Brito）是Coin Center的执行董事，Coin Center是一家参与联盟的比特币维权机构。他表示，越多的执法机构明白该项技术是如何工作的，那么他们就越能理解他们可以要求什么，以及应该如何要求帮助。他说数字货币目前在公众的印象，很容易让人想起互联网初期的时候，很多人都将互联网视为违法犯罪活动的中枢。正如该行业已经随着时间而改变，所以相信公众也会改变对比特币的看法。联盟需要做的是让公众明白，不应该因为犯罪分子使用比特币就认为比特币不好，而要做到这点首先就是把公众注意力拉回到数字货币的合法用途上。

12.美国联邦证券法监管机构对比特币或区块链技术发表意见

2015年11月，SEC委员卡拉·斯坦（Kara Stein）已针对围绕区块链技术和分布式总账技术的炒作发出了警告。她指出区块链技术近来受到越来越多的关注。此外，她还提到了区块链技术与比特币之间的关系，并列举了一系列目前正在探索的区块链技术应用，包括清算和结算、支付处理以及借贷交易。可以设想在一个世界中，证券借贷、回购和融资融券都是通过透明和公开的区块链来追踪交易。公共账本可能某一天会为政府监管者服务，能够让他们更好地监控金融市场中的“系统风险”。

虽然斯坦承认，这些应用可能会增加金融系统中的信任，但她同时也提醒到，这些想法目前仍处于“起步阶段”。此外，她相信这项技术也将通过监管机构、学术界以及资本市场参与者们的持续评估。而美国监管机构应紧密关注这项技术的发展，因为如果市场开始向区块链技术移动，监管机构需要处在一个引导的位置，利用它的好处并快速响应其潜在的弱点。

这是该美国联邦证券法监管机构首次对比特币或区块链技术发表意见。迄今为止，SEC参与行业活动，主要是针对倒闭创业公司的执法行动，例如GAW Miners以及Sand Hill交易所等。

13.DHS正在了解区块链技术

2015年12月，美国国土安全部（DHS）正在通过科学和技术部门（S&T）的小企业创新研究（SBIR）项目对区块链技术进行更详细的了解。其科学和技术部门副部长瑞金纳德·布拉德斯（Reginald Brothers）在一份声明中表示，要为国家国土安全面临的挑战广泛撒网，寻找高度创新的解决方案是非常重要的。因为美国小企业是具有创造性的问题解决者，也是创新的引擎，希望能从他们那里听到好消息。

现在，美国政府部门正在接受小企业的研究提案（在13个领域），包括“区块链技术匿名身份的适用性管理”和“区块链在国土安全分析方面的应用”。小企业创新研究（SBIR）项目分为三个阶段，旨在鼓励美

国小企业为联邦研究工作提供帮助，首先要评估提案的“技术优点和可行性”。

据透露，已经批准提案的第一阶段限时6个月，授予资金10万美元。而第一阶段通过后，进入第二阶段将有资格获得24个月的时间，以及高达75万美元的奖励。第三阶段是指在之前的SBIR资金资助下产生，扩展或完成的成绩，但这些资金是由发起者资助，而不是SBIR的项目资金。

在其他科学技术创新方面，国土安全部还进行了10个研究项目，其中包括紧急医疗服务的网络防御、实时数据分析研究以及恶意软件预测等。三笔拨款也正由国家核心探测项目办公室进行发放。

（二）欧洲

1.数字货币监管听证会

2016年1月，欧洲议会委员会在布鲁塞尔召开了一场数字货币听证会，讨论了近期巴黎恐怖袭击之后，监管数字货币的可能性。欧洲经济和货币事务委员会（Committee on Economic and Monetary Affairs, ECON）主持召开的听证会是该委员会随后发表数字货币报告的准备步骤。会议的议题包括：公共交易数字货币带来了风险和挑战，数字货币的基础——区块链和分布式总账技术对社会的影响。听证会的参加成员包括欧洲议会代表、经济合作与发展组织（OECD）代表、学术代表、私人领域的利益相关者。

在开幕式致辞中，德国MEP（Member of the European Parliament，欧洲议会会员）和委员会委员雅各布（Jakob Von Weiz Sackerm）重申了会议的目的，以及本次会议所做决议的重大潜在影响，因为政府对恐

怖主义融资的打击力度越来越大。雅各布表示，经过巴黎恐怖袭击之后，欧洲考虑是否需要数字货币进行监管。过去就已经考虑过这个问题，但在法国恐怖袭击之后，更需要研究可供选择的方法。

但是，他指出技术正在发展的过程中不应被过度监管，因为新技术有很多潜在的优势。监管顾问兼电子货币联盟CEO萨布里（Thaer Sabri）建议实行宽松的监管。

2.区块链将颠覆支付格局

2016年1月，欧洲央行（European Central Bank, ECB）执行董事会董事默施（Yves Mersch）认为诸如区块链的新兴支付技术很有可能破坏基于银行卡的支付系统。默施是在巴黎的一次法国银行会议中做出上述评论的，他当时演讲题目是《欧洲的卡支付——最新的趋势和挑战》。

当讨论到包括分布式总账技术等新兴支付技术的兴起时，这位银行家预测未来几年，新技术可能会对支付行为、卡的使用以及其他的传统支付工具产生影响。创新的卡支付服务取代了现金支付，它具有进一步增加卡支付的使用潜力。但警告卡支付行业将会受到来自创新支付服务的强烈挑战，后者的支付工具基础为非卡支付模式。

他预测分布式总账技术可能会对“整个金融生态系统产生深刻影响”，同时颠覆“传统”支付工具、支付服务和支付处理行业。消费者和企业有更多的选择是件好事，他认同新的支付方式安全、高效，而且所有的服务提供者“都遵循同样的规则”。

但是按照这位欧洲央行董事的看法，只要实现了瞬时支付系统，“并通过标准化，互操作性强和合适的安全措施”建立起一个“和谐的具有竞争力和创新的欧洲卡支付区域”，那么在欧盟区域内，卡支付交易还有“巨大”的增长潜力。不过他提醒银行业，上述创新式支付服务

将会对卡支付行业带来挑战。竞争将会来自基于SEPA（单一欧元支付区）的信用转账瞬时支付服务，来自电子商务领域的支付服务，以及来自分布式总账技术。

3.欧洲数字货币监管草案

在2016年2月，欧洲议会发布了数字货币监管草案，该报告由经济和货币事务委员会成员雅各布撰写。建议成立由自己预算和人员组成的专案小组，从事数字货币研究及为欧盟和成员国提供政策咨询。

欧盟委员会及其执行机构正在商讨这个提案。同时，欧洲理事会也在考量数字货币监管方案。在1月下旬的听证会上，议会成员们在恐怖主义融资和洗钱框架下讨论了比特币和区块链技术。之后，雅各布就发布了以上报告内容。

尽管呼吁加强数字货币活动监管，该报告认为，这项技术有推动经济发展和提高消费者利益的潜能。欧洲议会呼吁制定适当的监管条例，防止把技术创新扼杀在摇篮里，同时严肃对待数字货币和分布式总账技术潜在的政策风险。该报告力求获得对“迅速有力的监管措施”提议的认可，基于精确分析和权衡的这个监管政策不应与宽松的监管混为一谈。迅速有力的监管措施应成为政府工具的一部分，并能适时地阻止潜在风险的扩大。

经济和货币事务委员会会在4月对该报告内容进行投票，如果通过的话，最早5月就可以提请欧洲议会审核。

4.欧洲央行报告

欧洲央行已经公开宣布，正在探索如何将区块链技术为己所用。该声明是在2016年2月发布的一份名为《欧元体系的愿景：欧洲金融市场基础设施的未来》咨询报告中提到的。其中谈到如果将区块链技术应用

于该地区的证券和支付结算系统，他们将能够如何被改善。这份报告来自Target 2-Securities的出版物，Target2-Securities是一个在欧盟中整合结算和证券的全新平台，这表明联盟已经开始在研究这些技术问题。

欧洲央行负责欧盟欧元区的金融及货币政策，是为了适应欧元发行流通而设立的金融机构，同时也是欧洲经济一体化的产物。欧洲央行具有法人资格，可在各成员国以独立的法人资格处理其动产和不动产，并参与有关的法律事务活动。

5.新提议可重塑欧洲数字货币政策

在2016年2月，欧盟委员会（EC）宣布了欧盟反洗钱和反恐金融监管规划（反洗钱第四政令或4AMLD），该规划主要针对数字货币交易和可能的虚拟钱包供货商，属于欧盟委员会打击恐怖主义融资多项措施中的一部分。

欧盟机构曾经多次公开表述，要将数字货币纳入到反洗钱/打击恐怖主义融资（AML/CTF）的监管中——例如，欧洲银行业管理局在2014年发表过这样的言论，其他机构则在2015年2月和11月巴黎恐怖袭击后发言。似乎发生在巴黎的恐袭事件最终促使欧洲委员会采取监管措施。

虽然大家对这部规划的出台未感到任何意外，但欧盟委员会的另外一份提议，虽然宣传力度远远小于此规划，从某种程度上说是被人们忽视，但是它很有可能改变欧盟数字货币监管的现状。

除了扩展4AMLD范围，以覆盖数字货币交易的规划，欧盟委员会还粗略地介绍了另外一个监管理念，但媒体甚至都没有提及这个理念。如果执行该理念，其影响似乎更为深远。

欧盟委员会宣布他们将考虑使用支付服务指令的执照颁发和监督规

章（PSD，2015年已经实行了新版本，2PSD）来监管数字货币交易，以“更好地理解和控制市场”。

PSD是欧盟单一支付市场的奠基石之一。该规章为支付服务建立了规则，并包含支付服务的目录。提供支付服务的公司必须满足众多监管要求，包括执照颁发的监督规则，欧盟委员会打算将后者用于监管数字货币交易。

这种方案似乎比较合乎情理。很明显，欧盟中有两个法案非常适合监管数字货币：PSD和另外一个相关指令，E-Money指令（EMD）。目前欧盟正在制定新的“3EMD”，很有可能会对这部指令进行一些修改。

真正重要的是，目前的PSD监管方法是如何操作的。

PSD的一项关键部分是对“资金”的定义，目前已经将现金、银行活期存款和（受EMD监管的）电子货币纳入“资金”定义之中。数字货币不属于上述任何一项归类之中，欧洲央行和其他机构已经确认了此观点。

由于目前欧盟委员会的方案非常宽泛，所以很难对该方案做出评估，但是欧盟很有可能在欧盟支付服务监管中，准许数字货币进入。之后可能会涌现许多提议，从谨慎克制的提议到全面概括的监管提议。

（三）英国

1. 金融创新峰会

2013年9月4日在唐宁街10号，讨论监管比特币公司方案的会议召开。这次由第十政策组主办的金融创新峰会，出席的包括有来自众筹公司的支付服务行业、财政部、金融市场行为管理局（FCA）、第十政策组、创新和技能部，还有一些规模较小的银行。FCA说，他们正在积极

了解数字货币和研究如何对它进行监管。然而，会议并没有对如何采取决定设立一个时间框架。

FCA发言人表示，需要综合各方面考虑，虽然FCA并没有监管比特币，包括提供和比特币相关的商业模式，或者其他数字货币等，但应该考虑他们是否正在被监管的范围内。正如大家所期盼的，FCA正在密切关注这个市场中的新进展。

目前面临的主要一个问题是，不仅仅是数字货币企业，所有金融服务公司都很难找到合作的银行。监管机构目前的观点是这都取决于银行——他们有权利基于商业考虑做出不与公司合作的决定。但是，参与的公司都认为让银行做出这些“基于商业考虑”的决定就是因为他们被施加的监管框架。这个框架应该被改变了。

英国比特币基金分会目前已经到位，会根据比特币基金会的主要目标，专注于保护、促进和规范化在英国的比特币活动，也会代表比特币企业和用户来面对监管者和政府。目前正在等待比特币基金会说明在他们之间应该如何开展工作。

2. 税务海关总署

2013年11月，英国皇家税务海关总署似乎将要把比特币作为一种分类的凭证，这也就意味着增值税不久就会应用在所有交易上。英国皇家税务海关总署提出比特币应有纳税凭证，可以有一个增值税外汇免税交易，但问题是货币必须是法定货币。

3. 黄金比特币

从2013年夏季开始，英属奥尔得尼岛就一直在制订计划，与英国皇家铸币局合作发行实物比特币。这个仅有三英里长的小岛希望推出一系列符合反洗钱法规定的服务，包括汇兑、付款和比特币存储金库，进而

成为比特币的首个国际交易中心。这些特殊的比特币将成为该铸币局发行的一部分纪念币，其中包括限量版的硬币和邮品。这类比特币铸造时会加入黄金成分，预计每一枚价值500英镑。所以，如果这些比特币的兑换价值暴跌，持有者可以熔化它们，出售其中的黄金。这样看来，奥尔得尼岛筹划的或许可以视为一种得到黄金价值支持的比特币。

若消息属实，这可以算是一场革命，因为它是首次由一个国家的财政部/央行暗示愿意将比特币变为法币，并且是将象征性的比特币用作商品。这项计划还没有最终确定，英国皇家铸币局自然也不急于披露计划的全部细节。英国皇家铸币局的新业务负责人戴维·简泽威斯基（David Janczewski）确认，奥尔得尼财务部部长曾与他商讨，探索有无可能制造一种比特币题材的实物纪念币。但讨论还没有更深入地进展，这个阶段依然只是概念而已。

实物比特币发行机制是这样：一家独立的公司A提供比特币。如果比特币价格暴跌，奥尔得尼和英国皇家铸币局都不会受到任何损失。A公司会以协议价格将比特币存于一个第三方保管的账户。同时，英国皇家铸币局会根据客户的订单得到铸造的比特币，利用发售硬币获得收入。支持实物硬币的虚拟比特币将以数字形式存在奥尔得尼的设备中。英国皇家铸币局会发行纪念币形式的比特币，出资购买这类比特币内含有的黄金。奥尔得尼出售这些硬币就可以收取使用费。上述硬币比特币可以任何时间在奥尔得尼兑换为英镑，价格以兑换日的比特币汇价为准。

4.放弃征税

2014年3月，英国税务局表示准备放弃对比特币交易征税的计划。英国税务海关总署（HM Revenue & Customs）表示，它不会对相关交易征收20%的增值税（VAT）。此前创业家抱怨称，增值税使他们的业务在全球缺乏竞争力。英国税务海关总署进一步表示，也不会对他们的

保证金征收该税。这一裁定回避了是否把比特币界定为一种货币的问题，但实际上是把它当作一种货币；裁定的依据是欧盟有关对“可转让票据”的支付和转让免予征税的法律。

相信2015年最为重要的司法监管制定来自英国。在回答征求意见时，英国财政部在2015年3月宣布，计划要求英国的数字货币交易所和其他受监管的金融中介机构一样，开始实施反洗钱标准。然而，这一更严格的要求（如最低资本要求等）仅仅适用于某些提供保管业务的金融服务企业，并且也是一个可选项。托管人将不会被法律强制要求满足这些条件，但是那些能做到的将会获得一个类似于鼓舞信心的“审核印章”，由英国标准协会（British Standards Institute）进行颁发。

5.英国政府报告

2016年1月19日，英国政府发布了一份关于区块链技术的重要报告。这份名为《分布式总账技术：超越区块链》的报告指出，英国联邦政府和政府首席科学家马克·沃尔彼特（Mark Walport）将会投资区块链技术来分析区块链应用于传统金融行业的潜力。

该报告认为，去中心化账本技术在改变公共和私人服务方面有着巨大的潜力。它重新定义了政府和公民之间数据共享、透明度和信任，将会主导政府数字改造规划方案。任何新技术肯定都会带来挑战，但是如果能够很好地处理领导、协作和治理之间的关系，分布式总账能为英国带来很多好处。

除了创建一个基于区块链的公共平台来为全民和社会提供服务外，英国政府还计划开发一个能够在政府和公共机构之间使用的应用系统。沃尔波特和他的研究小组，将会协作将分布式总账技术集成到政府管理中，保证政府的隐私和安全。

不过，英国政府现在试图建立的分布式总账系统，将会在他们区块

链网络中实施他们自己的“规则”。英国政府强调，使用数学方式来保护区块链网络的思想是一种“误解”，政府应该参与数字货币和区块链网络的立法是非常重要的。

6.英国央行的新蓝图

主管金融市场与银行业的英国央行副行长米南克·沙菲克（Minouche Shafik），在2016年1月有关支付行业的演讲中表示，近年来支付方式已经发生了巨大的变化。沙菲克指出这些变化主要由新进入的支付供给商数量激增与对支付基础设施的需求变化两个因素所驱动。她指出无现金实时移动支付方式的可选范围将持续增加，以及分布式总账技术实现了支付验证的去中心化。在她看来，成立于2015年的支付系统监管部（PSR）对于支付行业的监管正在从有针对性的干预措施向更加动态关注竞争和创新方向转变。

英镑结算的未来发展与每个英国人都息息相关。实体经济中的绝大多数支付——无论是从工资到发票，从购买汽车到售卖咖啡，从养老金到投资——最终都要依靠已经“20岁”的银行实时全额结算系统（Real-Time Gross Settlement, RTGS）服务来解决。根据银行业数据，RTGS的每日结算规模为5000亿英镑，几乎是英国每年国内生产总值的1/3。“所以毫不夸张地说，实时全额结算系统是英国支付系统的核心。”

2014年10月20日，实时全额结算系统崩溃，中断服务9小时，数百亿美元的支付交易被推迟。银行需要额外4个小时的时间来应付所有未完成的交易。2015年3月25日，英国央行公布了德勤有关2014年10月20日实时全额结算系统中断服务9小时问题的独立审查结果。银行接受了所有的审查建议并表示将进一步考虑该系统的应急方案以及其未来的发展。

回到现实，考虑到实时全额结算系统的重要性，沙菲克指出在追求金融稳定过程中系统的修复能力再怎么强调都不为过。对于人们付款和

收款能力的持续性破坏将对英国经济造成巨大的损害。因此，英国央行正在寻求支付系统的创新支持。

沙菲克提出了有关英国支付系统新蓝图需要解决的四个首要问题。第一，在涉及央行货币结算中英国央行的政策目标；第二，英国高性能的支付系统的具体功能；第三，支付系统的具体参与者与参与方式；第四，在支付系统服务中英国央行的作用。

沙菲克强调，当央行对于未来10年或者更长时间的支付系统进行投资决策时，应要求其能够应对用户需求变化，需要有一定的“选择权”，其能够使我们应对世界的不同状态。

英国央行表示，其将设计一个有关英镑结算系统的新蓝图来适应未来需求。在进行小规模的专业咨询之前，英国央行将在前期进行涵盖各方的更广泛的讨论。而且在2016年年底，将对有关高性能英镑结算系统新蓝图达成一致，同时2017年也将提出有关技术进步的新蓝图方案。

创新和稳定能够携手前行。英国央行面临的挑战将是寻求重新设计RTGS的最优路径，该路径能够在实现系统弹性提升的同时又能促进技术创新有益于公众利益。期待分布式总账技术等创新，能够解决银行结算业务形态的基本问题。

7.发行数字货币

2016年1月2日，英国央行总出纳维多利亚·克莱兰（Victoria Cleland）对BBC（英国广播公司）表示，英国央行正在研究是否应当发行数字货币。克莱兰说，央行正在考虑，可否使用数字货币，为人们带来与纸币同样的安全和保障，但研究工作正处在相当初级的阶段。克莱兰还补充说，公众对现金有非常旺盛的需求。英国零售商协会过去进行的研究显示，使用现金的成本很低，因此零售商在考虑消费者的需求之外，也会考虑成本的问题，部分零售商会非常青睐现金。

2016年3月，英国央行与伦敦大学学院研究员合作，开发央行控制的数字货币。最新的RSCoin用密码学技术打击造假。与比特币底层区块链技术不同的是，RSCoin由中央机构控制。英国央行宣布发布数字货币RSCoin代码并进行测试。

2015年的一份文件显示，伦敦大学学院研究员莎拉·米克尔约翰（Sarah Meiklejohn）和乔治·达纳齐（George Danezis）预测，RSCoin的货币政策会由央行控制。该技术将依赖于一系列权威机构，如商业银行防止货币重复消费。央行完全控制货币供应，同时依赖于一些机构来防止货币重复消费。不过，尽管RSCoin的货币政策由中央监控，其仍然有很高的透明度和可审计性保证。

开发RSCoin的目的，不仅是寻求受央行控制的可扩展数字货币，也是给更多的央行提供数字货币部署的框架。比特币及其他现有数字货币的缺点是缺乏扩展性，研究员认为这是个亟待解决的问题。比特币每秒最多处理7次交易，并且面临“提高速度的巨大挑战”，因为无法达到计算机算力要求。

2016年4月，英国内阁大臣马特·汉考克（Matt Hancock）说，政府在研究区块链技术管理和追踪公共资金的途径，例如学生贷款和补助等；认为区块链可以“培养新的信任文化”。他认为政府不能逃避现实并忽略新兴科技的发展，过去政府也曾这样对待互联网，这次我们不能旁观这种事情再次发生。

英国政府IT系统曾经出现过漏洞，影响了护照机构、税收信用体系，并且最重要的是2011年英国国民健康服务体系（National Health Service, NHS）曾被迫宣布放弃几十亿英镑的病历电脑化存储项目。同时汉考克也警告不能陷入区块链炒作的陷阱，他认同区块链不能解决所有问题，也并不适合所有应用场景。

（四）俄罗斯

1.意欲严惩比特币活动

俄罗斯联邦财政部作为国家经济法律制度部门，已经在2015年中反复强调反对允许比特币代替国家发行的货币。在2015年10月，俄罗斯财政部副部长阿列克谢·莫伊谢耶夫（Alexey Moiseev）曾经公开表示，财政部正在着手拟订法律草案来处罚将数字货币转换成卢比的行为，最高可获4年的刑期。除了这些主张外，财政部对比特币作为金融技术的态度并不很明确。

俄罗斯政府已经意识到了区块链技术对虚拟经济发展的潜在关系，因此觉得它应该被允许和发展，但比特币本身特别是比特币交易在实体经济和银行系统的实施会十分危险。但在俄罗斯可能正在关注比特币转化入罪的同时，莫伊谢耶夫表示不认为比特币是对俄罗斯国家货币的威胁。

虽然没有成功预示这个技术在俄罗斯会怎么被监管。俄罗斯央行已经表示反对比特币的使用为不合法的措施，在2015年7月第一次讨论数字货币的时候，普京已给予支持。当时，普京支持俄罗斯银行对这个技术的提议，但暗示比特币没有任何实体支持，因此可能要求特别的监督。

虽然比特币的未来在俄罗斯仍然不明朗，但可能安全的说法是密码学爱好者至少现在可以放松。财政部意欲使比特币转换入罪的法律草案正在被内阁审议，这个进程可能会持续几个月，然后会被提交到国会得到最终的通过。

2.俄罗斯央行研究区块链

2016年2月，2014年被任命俄罗斯央行副主席奥尔加·斯罗博格国娃

（Olga Skorobogatova）告诉俄罗斯银行业代表，俄罗斯央行认为，当全球越来越多金融机构都开始采用区块链技术时，区块链应用会在未来金融领域中扮演一个非常重要的角色。

斯罗博格国娃认为，2017~2018年将会看到该系统的实际案例被使用。作为一个自成体系的系统，（区块链）就是未来，需要为此做好准备。俄罗斯已经打算开始立法规范所谓的“货币代理”，特别是指某种非政府发行的货币，包括比特币和其他数字货币。

然而，目前真正的问题是俄罗斯打算如何去真正禁止任何涉及数字货币的活动。与此同时，俄罗斯的一些私人企业已经开始探索该项技术的应用，该国支付公司Qiwi已经宣布它打算发行自己的某种数字货币。

尽管俄罗斯此前对数字货币持消极态度，但现在开始支持“对比特币保持谨慎态度并看到它的经济潜能”。另外，尽管俄罗斯财政部承认了区块链技术在金融业的潜在作用，但它的一系列声明却都是在谴责比特币本身。

（五）德国

2013年8月，德国政府认可了比特币的法律和税收地位，成为全球第一个正式认可比特币合法身份的国家。

德国财政部是在回应该国议会金融委员会成员弗兰克·舍弗勒（Frank Schaeffler）的询问时认可比特币身份的。其在声明中表示，比特币没有被归类为电子货币或者外汇，但它是一种在德国银行业条例下的金融工具。它与“私人货币”更为接近，可以用来进行多边结算。这意味着比特币在德国已被视为合法货币，并且可以用来缴税和从事贸易活动。此前，德国议会曾决定持有比特币一年以上将予以免税。如今德国财政部认可比特币为一种“货币单位”和“私有资产”，这也就意味着与比

特币相关的商业活动盈利将被征收税款。不过，个人使用比特币仍享受免税。

（六）瑞典

2013年9月4日，某瑞典比特币用户在LocalBitcoins网站售出5个比特币以后，钱已经存到用户的银行账户，几天后，当用户查看银行账户的时候，已经被冻结，不能进行任何操作。银行在冻结用户的银行账户15天以后才解冻。一位瑞典银行发言人说，目前用户不禁止用户进行比特币交易，然而，特殊的境况需要特殊对待。瑞典银行的监管部门认可并接受比特币。

瑞典比特币交易网站Safello CEO弗兰克·斯古伊尔（Frank Schuil）指出，目前瑞典本地人很少在LocalBitcoins上进行比特币交易。但他认为，在瑞典“创新是接受而不是拒绝”，相信比特币在瑞典能够蓬勃发展。

（七）瑞士

2013年9月，瑞士联邦议会一名瑞士社会党成员向该国的国民议会提交了一份申请，要求写一份关于比特币的报告。他认为通过比特币的洗钱和其他犯罪活动将会对瑞士产生危害。但是，他承认，数字货币对国家也有益。他说比特币的出现引起了他的注意，因为自己对互联网政策、数据保护和新的网络趋势有着浓厚的兴趣。他作为银行工会会员工作时还遇到过比特币——他现在在瑞银雇员协会执行委员会工作。

这位瑞士工会会员还认为，90%的瑞士议会成员根本不知道什么是比特币，大多数政府也不知道，因为它太新了。但是瑞士记者可以从丝

绸之路使用比特币购买到药物，所以国家需要进行干预。虽然并不确定什么样的干预是必要的，但他说，第一步是为政府做一些研究和评估它可能会造成的危险性，以及其优势和机会。在那之后，就可以决定哪些措施是必要的——比特币是否应该被禁止或监管，如果这样的话，瑞士可以单独订立规则，或与其他国家合作建立监管。

2014年6月，瑞士联邦委员会出版报告阐明，暂时不会对比特币或其他数字货币进行立法限制。政府报告声称目前数字货币在经济体系里是毫无意义的，理事会不希望改变其未来。

政府报告的一个要点是并不存在数字货币的法律真空，意指现行法律体系适用于数字货币。报告认为，“现行的针对货币的合同在原则上也可用于处罚虚拟货币的犯罪行为。基于虚拟货币的商业模式也受制于金融市场法律，需要服从金融市场监管……虚拟货币贸易及交易平台在瑞士一般要受反洗钱法案监管，包括遵照法律识别缔约方的身份和收益人的身份。”

适用于数字货币的其他法律和可受制机构还包括瑞士债务码条约，管理恐怖主义财务的联邦法院，以及联邦银行和储蓄银行法庭。报告列举了比特币有关的风险案例，但对国家财政没有构成威胁，消费者要注意其安全性，并劝告使用比特币的用户建立消费者权益保护组织。

2015年6月，瑞士联邦税务局（ESTV）决定，在瑞士使用比特币不需要缴纳增值税。税务局意识到比特币就像瑞士法郎那样，是一种支付方式，但没有保值功能。因此，数字货币的转换并不构成货物的传送，也没有所谓的增值税的征收。同时，把电子货币转换成瑞士法郎就像是把法郎兑换成欧元。而且在瑞士增值税法案的第二十一条第二节中可以看到，比特币公司所需缴纳的交易费用被免除。所以，比特币是不需要缴纳增值税的。

考虑到瑞士良好的发展环境及法律法规，包括钱包服务供应商，交

易及咨询公司在内的许多比特币初创公司在过去几个月中开始迁往瑞士。著名的区块链项目——以太坊的基金会也把总部设在了瑞士。

（八）中国

1. 首谈比特币

2013年11月，中国人民银行副行长易纲在某论坛上首谈比特币。易纲表示，从人民银行角度来看，近期不可能承认比特币的合法性。但他同时认为，比特币交易作为一种互联网上的买卖行为，普通民众拥有参与的自由。此外，易纲还指出比特币“很有特点”，具有“启发性”，个人会保持长期关注。有经验的观察家则总结认为这是一个积极的信号，因为易副行长的话中暗示出中国政府不会将比特币判定为非法。此外，易副行长也承认购买和出售比特币是公民的权利。基于上述评论和新闻，我们也许可以对比特币在中国的未来做出乐观的推测。

2013年11月19日，《人民日报》发文《比特币虽火，冲击力有限》，对目前比特币的火热现象进行评论，分析人士认为这一定程度上反映了目前中国官方对于比特币耐人寻味的态度。

比特币虽是迄今为止最为高级的形态，但正如美国一名联邦法官所表示的，比特币只是“一种货币或一种形式的资金”，目前其金融属性或许要高于货币属性，因此对于整个货币体系的冲击还非常有限.....以现代货币的标准来看，比特币尚未充分满足货币的定义.....数字货币的出现，是一种草根服务创新，适应了互联网时代的货币需求。不过，如果数字货币规模达到一定程度，并积累了系统性风险，那么自然会受到监管部门的关注。

2. 五部委通知

2013年12月5日，中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会日前联合印发了《中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会关于防范比特币风险的通知》。

中国人民银行并非全世界第一个注意到比特币的政府监管机构，但却是第一个以发“公文”的形式对比特币的发展提出规范的。该《通知》发出后，各大交易网站上的比特币价格瞬间跳水：Mt.Gox价格从当日最高1240美元最低跌至870美元；BTCC（比特币中国）价格从当日最高7050元人民币最低跌至4521元人民币。不过随后两大交易网站的价格都有所回升，分别为1080美元和6106元人民币。

3.数字货币研讨会

2016年1月20日，中国人民银行数字货币研讨会在北京召开。来自人民银行、花旗银行和德勤公司的数字货币研究专家分别就数字货币发行的总体框架、货币演进中的国家数字货币、国家发行的加密电子货币等专题进行了研讨和交流。

会议指出，随着信息科技的发展以及移动互联网、可信可控云计算、终端安全存储、区块链等技术的演进，全球范围内支付方式发生了巨大的变化，数字货币的发展正在对中国人民银行的货币的发行和货币政策带来新的机遇和挑战。中国人民银行对此高度重视，从2014年起就成立了专门的研究团队，并于2015年年初进一步充实力量，对数字货币发行和业务运行框架、关键技术、发行流通环境、面临的法律问题、对经济金融体系的影响，法定数字货币与私人发行数字货币的关系，以及国际上数字货币的发行经验等进行了深入研究，并已取得阶段性成果。

在中国当前经济新常态下，探索央行发行数字货币具有积极的现实意义和深远的历史意义。发行数字货币可以降低传统纸币发行、流通的

高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力，更好地支持经济和社会发展，助力普惠金融的全面实现。未来，数字货币发行、流通体系的建立还有助于我国建设全新的金融基础设施，进一步完善我国支付体系，提升支付清算效率，推动经济提质增效升级。

中国人民银行数字货币研究团队将会积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，建立更为有效的组织保障机制，进一步明确央行发行数字货币的战略目标，做好关键技术攻关，研究数字货币的多场景应用，争取早日推出央行发行的数字货币。数字货币的设计应立足经济、便民和安全原则，切实保证数字货币应用的低成本、广覆盖，实现数字货币与其他支付工具的无缝衔接，提升数字货币的适用性和生命力。

中国人民银行在推进数字货币研究工作中，与有关国际机构、互联网企业建立了沟通联系，与国内外有关金融机构、传统卡基支付机构进行了广泛探讨。参与研究的国内外人士高度重视此项工作，并就相关的理论研究、实践探索及发展路径与人民银行系统的专家进行了深入交流。

4.再谈数字货币

2016年2月，央行行长周小川在接受媒体采访时畅谈了数字货币的未来。周小川表示，从历史发展的趋势来看，货币从来都是伴随着技术进步、经济活动发展而演化的，从早期的实物货币、商品货币到后来的信用货币，都是适应人类商业社会发展的自然选择。作为上一代的货币，纸币技术含量低，从安全、成本等角度来看，被新技术、新产品取代是大势所趋。

周小川还介绍说，数字货币作为法定货币必须由央行来发行。数字货币的发行、流通和交易，都应当遵循传统货币与数字货币一体化的思

路，实施同样原则的管理。央行发行的数字货币目前主要是替代实物现金，降低传统纸币发行、流通的成本，提高便利性。

央行将运用包括密码算法在内的多种信息技术手段，来保障数字货币的不可伪造性。未来的技术也会有升级换代，央行会提前将技术升级考虑在内，从最初就引入长期演进的发展理念。对于央行掌控的数字货币，会采用一系列的技术手段、机制设计和法律法规，来确保数字货币运行体系的安全，一开始就与比特币的设计思想有区别。

周小川的讲话还传递出一个明确信号：推出数字货币没有时间表。中国人口多、体量大，像换一版人民币，小的国家几个月可以完成，中国则需要约十年。所以数字货币和现金在相当长时间内都会是并行、逐步替代的关系。

周小川介绍说，数字货币的技术路线可分为基于账户和不基于账户两种，也可分层并用而设法共存。区块链技术是一项可选的技术，其特点是分布式簿记、不基于账户，而且无法篡改。如果数字货币重点强调保护个人隐私，可选用区块链技术，中国人民银行部署了重要力量研究探讨区块链应用技术，但截至目前区块链占用资源还是太多，不管是计算资源还是存储资源，应对不了现在的交易规模，未来能不能解决有待观察。

实际上，要实现数字货币化并非易事。如何在安全性、便利性等各个方面都能够解决所谓价值交换需要的功能载体，这有很多技术问题需要解决；技术问题解决后，未来如何运用数字货币替代纸币的流通和发行，需要一个循序渐进的过程。

除了应对现有数字货币的挑战之外，更有央行人士提出了推动SDR（特别提款权）基于分布式规则的数字化，也应该成为改革现有货币体系的尝试。

中国人民银行金融研究所所长姚余栋撰文认为，或许可以跳出陷入困局的现有发行机制，在IMF和成员国的共同努力下，探索建立“全球央行”的机制雏形，并尝试基于数字货币规则的创新，即eSDR。

2016年6月15日，中国互联网金融协会（NIFA，NATIONAL INTERNET FINANCE ASSOCIATION OF CHINA）决定成立区块链研究工作组，由全国人大财经委委员、原中国银行行长李礼辉任组长，深入研究区块链技术在金融领域的应用及其影响。

中国互联网金融协会（national internet finance association of china，英文缩写NIFA）是按照2015年7月18日经党中央、国务院同意，由中国人民银行会同银监会、证监会、保监会等国家有关部委组织建立的国家级互联网金融行业自律组织。

区块链工作组为中国互联网金融协会领导下的专项研究组织，将重点对区块链在金融领域应用的技术难点、业务场景、风险管理、行业标准等方面开展研究，跟进国内外区块链技术发展及在金融领域应用创新，密切关注创新带来的金融风险 and 监管问题。

研究工作组的主要工作目标包括：构建区块链研究网络，规划建设区块链基础实验平台，形成高水平的研究成果，培育高层次、复合型专业人才。研究工作组将积极借鉴国际经验，开展学术交流，注重研究成果转化应用。

（九）中国香港地区

1.不监管比特币

香港地区金融管理局（金管局）首席长官陈德霖发布公告称，将不会监管比特币。不过也表示，金管局有责任“促进金融体系的稳定性和

完整性，包括银行体系”，但不适用于比特币的监管。按陈德霖的说法，以钱的形式来描述比特币此类数字货币并不恰当，由于比特币受价格波动影响太大，虽然有人投资比特币，但比特币作为支付媒介并不稳定。

金管局相信比特币在香港的使用并不广泛，但当局一直在监视人们如何使用它，关注它的价值。虽然做出了不监管的表态，但当局仍会密切关注其他国家对其的监管要求与其他相关发展。被提及的还有最近发生的比特币期货交易平台GBL卷钱跑路事件，呼吁香港监管机构必须采取措施，避免类似事件的雪球效应的发生。

香港财政司司长曾俊华在2013年12月1日表示，比特币仍不算上是电子货币，只是可以进行私人或网上交易的“数字货币”。虽然有公司愿意收取比特币，以交换货物或服务，但规模仍然微不足道，而且由于比特币的价格波幅非常大，这些公司愿意收取比特币，似乎很大程度是憧憬比特币会继续升值，多于节省交易成本等实际经济考虑。现在比特币的投机成分很高，市民考虑投资比特币、商店考虑收取比特币进行交易时，必须加倍小心，必须了解相关的风险。他同时鼓励年轻科技人才开发比特币应用程序。

2015年3月，香港政府曾经表示过一定程度的担忧，认为严厉的监管将会严重打击数字货币。随后公布的官方态度表明，比特币“对于金融体系尚不构成显著威胁”。金融服务和财政部部长得出结论：“没有必要通过立法来监管虚拟商品交易，或者禁止人们参与这样的活动。”香港是数字货币活动的中枢地区，这个确定的监管说明为企业运营提供了一个迫切需求的稳定环境。

2.政府财政预算案涉及区块链

2016~2017财政年度香港特区政府的政府财政预算案的“新经济秩序”一章里，专门在金融科技这一部分中提到了区块链技术。

香港特区政府财政预算案的言辞指出：“政府会鼓励业界和相关机构，探讨区块链技术在金融业的应用，发展其减少可疑交易和降低交易成本的潜力。香港会通过培育计划，向业界提供培训，推广有关技术，发展更多服务和产品。”

香港特区政府是世界上首个在财政预算案中明确提到区块链技术的政府部门。作为亚洲乃至全球最重要的金融中心之一，香港在金融科技上对区块链一直保持着高度的关注。区块链技术作为一种有潜力重塑下一代金融体系的重要技术之一，已经受到了不少重量级机构的关注。除此之外，该预算案中还提到以下内容：“金融科技通过运用流动通信技术、人工智能等科技，为消费者带来全新的理财体验，提升金融机构的营运效率。金融服务提供者不再局限于银行和保险公司等传统金融机构。电信公司、电子商贸企业和初创企业都能借着互联网和移动科技，为个人和企业提供金融服务”。

3.努力追赶区块链技术

2016年4月，香港应用科技研究院（ASTRI）表示，特别行政区的许多金融机构不了解比特币的底层技术。该组织机构将会通过使用基于区块链技术的应用程序加强参与度，这些应用程序包括为移动电话和近场通信（NFC）行业提供不同的解决方案。

ASTRI由香港特区政府于2000年成立，其使命是要通过应用研究协助发展以科技为基础的产业，借此提升香港的竞争力。2006年4月，ASTRI获创新科技署委托，承办“香港资讯及通信技术研发中心”，肩负进行高质素研发使命，把科技成果转移给业界；培育优秀科技人才；整合业界和学术界的研发资源等任务。ASTRI锐意创造世界级顶尖科技，实践以顾客为导向的应用研究，以配合业界的真正需要。研究范畴横跨五个相关领域，并于最近成立“信息研究室”，针对新兴和跨领域技术进行研究。

ASTRI表示，区块链技术已经证明了自己能够给银行和金融业带来改变。如果中国香港想和伦敦、纽约这样的金融巨头并驾齐驱，就必须尽快改革。比特币技术除了用于执行和记录比特币交易，还用于许多其他目的。虽然香港有许多比特币公司，但是比特币技术还没有完全被开发。ASTRI科学数据与信息安全总监表示，比特币区块链技术能保证交易的及时性。比特币区块链的透明性能让每个人都能看到，这可以有效防止洗钱和其他非法交易。人们绝对想不到能够在这样的平台做交易，这是平台让每个人也能访问，有些人也会在平台中指出交易信息的偏差。

（十）日本

1.数字货币监管

2015年11月，日本国内金融服务中心的成员——日本最高金融监管者——正在为比特币相关企业起草监管大纲。日本政府在之前就已经暗示，要加强对比特币企业监管的力度，以应对Mt.Gox公司的倒台。

2016年2月25日，日本监管机构提议将比特币等数字货币作为一种支付方式。这样数字货币在法律上将等同于日本传统货币。而日本金融厅（Financial Services Agency, FSA）正考虑是否修改相关法律条文，将数字货币划入“具有货币功能”的类别。

按照日本金融厅的解释，数字货币应作为交换媒介，也就是用于购买物品和服务。数字货币应当可以在贸易和商品交易活动中兑换成法定货币。在这种环境下，金融机构应当在日本金融厅注册。相关监管机构认为，这样可以避免出现类似Mt.Gox公司的情况。2014年，这家日本比特币交易公司损失了几百万美元，并破产倒闭。但日本监管机构也的确面临一个两难的抉择，如果不把数字货币等同于货币进行管理，则数字

货币可以完成许多货币所不允许完成的功能，这会让资金监管出现一个很明显的漏洞。但是如果把数字货币看作货币，也会面对许多法规上的问题，特别是等于给予了数字货币法定货币的待遇，也有可能会造成金融市场上的混乱，并且还会需要对许多目前的金融法规进行修改。日本又是几乎唯一一个出现过大型数字货币交易所倒闭事件的国家，这让监管机构不得不抱着极其谨慎的态度。

日本经济产业省（Ministry of Economy Trade and Industry, METI）一直在讨论区块链技术对于国内金融业的潜在影响。根据METI2015年10月16日互联网金融研究小组会议记录，政府机构已经意识到，美国已经把区块链技术和分布式总账视为金融技术的一部分，并且引起了很广泛的兴趣。METI最新的会议纪要显示，与会者普遍认为，区块链技术有可能会对“整个金融行业产生影响”，且它的影响是巨大的，且它的重要程度类似于互联网和谷歌的出现。该文件还指出，在会议上建议区块链技术可以为金融机构显著降低成本。尽管如此，会议上METI围绕着技术进行了多方的沟通，与会者还在会议中讨论了比特币交易中存在的信誉和洗钱等潜在安全问题。

2. 谋求亚洲技术领导者

FSA代表认为亚洲应该作为区块链技术的领导者。

2016年3月，在东京OECD-ADBI（经济合作与发展组织—亚洲开发银行研究院）圆桌会议上，关于资本市场和金融改革的专题报告中，国际事务副部长马莎米奇·科诺（Masamichi Kono）认为在讨论区块链技术之前亚洲需要借助新型科技。他表示，亚洲的优势之一就是可以充分利用科技创新。特别是对于这些“颠覆性”科技，如分布式总账和区块链技术，亚洲有很强的竞争优势，并且可以为亚洲配置一些新工具，用更便宜且安全的方式来促进经济增长。

科诺表明FSA相信会把增加市场信息当作首要任务，但是也会支持

可以提高透明度和责任的技术，同时加强会计创新和公司治理。对于2008~2009年的金融危机，亚洲金融系统就如何转变的问题进行了广泛的讨论。科诺表示市场正在从“过度依赖少数银行”转变。

最新的一些声明表明了日本最高金融管理者不仅担当了行业领导者的角色，还发布一系列声明表明准备在现存的法律和框架中引入比特币和数字货币。例如，FSA最近提交了议案，关于国内经济管理条例对日本国家立法机关带来的改变。这个定义能让比特币变成一种资产，由此给交易所引进了反洗钱（AML）和了解客户（KYC）的规则。

3. 首个区块链行业组织

2016年4月，日本已经成立了首个区块链行业组织——区块链合作联盟（BCCC）。该组织由三十几家对研究开发区块链技术感兴趣的日本公司组成，其目的是要增加区块链技术在日本的关注度。

BCCC主席柿谷平野（Yoichiro Hirano，Infotera有限公司首席执行官）4月25日在日本新闻发布会上宣布该联盟正式成立。柿谷平野表示，区块链技术不仅仅因为是互联网金融核心而受到大众欢迎，同时还因为其推动了每个行业信息系统的改革。在该联盟形成之前，区块链相关的成就和信息在日本是不会共享的，所以应用程序的应用范围是受到限制的。因此，这些相信区块链未来潜力的人，想通过共享信息、公平竞争、推广区块链技术、积极扩展区块链应用程序的应用范围、提供资金支持区块链研究的方法，来保持日本竞争力以及促进区块链技术的发展。BCCC将和世界上其他区块链组织进行合作，会把从海外学到的知识应用到本国中，作为区块链技术的先驱国家，也会把专业知识和经验分享到全球。

联盟成员公司会成立以下小组委员会，同时会在合适的时候参加活动来推广巩固区块链技术。

- 大众化小组委员会：促进区块链技术的推广，举办如会议和研讨会的推广活动。

- 实践应用小组委员会：加速区块链应用于其系统和服务，公布实际应用案例。

- 技术小组委员会：加强对区块链技术的了解，培养对区块链技术感兴趣的工程师。

- 管理小组委员会：管理整个联盟及审查政策。

（十一）新加坡

2014年1月，新加坡国内税务局（IRAS）表示，在新加坡注册的公司进行比特币买卖或用数字货币换取商品和服务的交易须纳税，比特币交易须征收7%的增值税。

当比特币用于支付商品和服务时，这些交易被视为实物交易，因为比特币不是由政府认可的货币。因此，可以对所有比特币及产品和服务的交易征收增值税。如果数字货币在虚拟的游戏中使用是不征收增值税的。增值税征收数额取决于公司是否充当代理人或交易的主体。因此，如果代理他人公司进行比特币交易——这种比特币交易是把货币转移到用户钱包里——这种情况只对佣金征收增值税。

但是，如果一家公司作为委托方，如果给用户提供比特币的买卖服务，那么需要对所有的款项征收增值税，包括佣金。IRAS强调未在新加坡注册的公司进行比特币的相关服务不在增值说的征收范围。

2015年11月，新加坡总理李显龙督促该国银行和监管机构跟上技术的发展，特别提到区块链技术。在新加坡大华银行成立80周年的晚宴

上，李显龙总理提到了金融行业目前所面临的挑战，并强调跟上技术发展的步伐，用以保持竞争力。他说：“展望未来，银行业正在进入一个全新的挑战……经营环境变得更具挑战性，但最重要的是，技术推动层出不穷的全新商业模式来破坏银行的原有业务。例如，越来越多的人通过智能手机进行支付。”

李显龙总理还特别强调：“……还有一些其他新技术，就如区块链技术，它目前被用于比特币，但是也能够应用在其他领域，比如实时全额结算，或者是金融交易确认。所以我们的银行和监管机构必须要能够跟上，能够赶上发展的脚步。”尽管行业目前面临着许多挑战，李显龙总理也说银行过去一直处于强势地位，但是不要自满，要持续地关注变革机会。“我们处于亚洲崛起的心脏地带，银行有强大的资产负债表，并且有很强的区域存在，在周围有许多机会可以利用，但是也需要明白这是一个充满竞争的业务，并且始终在快速发展。因此他们必须提升自己的技术、服务和商业模式。”尽管他极大地褒奖了新加坡的银行业，但是他也特别指出，某些海外银行及其推广各自数字银行的模式非常“杰出”。

2015年12月底，新加坡资讯通信发展局（Infocomm Development Authority of Singapore），宣布联手新加坡星展银行和渣打银行共同开发首个发票金融（Invoice Financing）的区块链应用，将用于让发票金融贸易变得更加安全和简单，包括对企业和放贷银行。尽管这个用于加强发票融资贸易安全性的首个应用程序还处于概念阶段，而且使用范围也很有限，但是新加坡政府正在努力将自己打造为“智能国家”（Smart Country），这肯定是其中重要的一步。

（十二）澳大利亚

澳大利亚标准局——澳大利亚标准协会（Standards Australia）呼吁

国际标准组织ISO制定有关区块链技术的国际标准。澳大利亚标准协会是全球160家ISO公认的国家标准组织成员国之一。

总部设于日内瓦的国际标准化组织，是全球公认的最权威的标准组织。近日，其会员国澳大利亚呼吁制定区块链技术国际标准，该技术为比特币提供支持。

澳大利亚标准协会首席执行官阿德里安奥康（Adrian O’Connell）于2016年4月提出观点，认为该分布式分类账技术需要ISO标准认证。他指出，全球区块链交易者之间的互操作性将是解锁区块链技术潜能的关键。这需要国际化标准来帮助它解锁潜力，最佳选择就是通过ISO组织。

值得注意的是，ISO组织规定，提议只要获得五个成员国的一致同意便可通过。因此，该提议极有可能通过ISO组织。

通过寻求ISO组织设立区块链技术委员会，能够越来越清楚地表明澳大利亚对该领域抱有极大兴趣。尽管全球银行都在R3财团、股票交易所、服务机构和医疗保健公司这些不同的领域研究和发展的分布式分类账应用，但是阿德里安奥康指出，仍然缺乏互操作性国际标准促进创新。

尽管目前有许多组织在开发区块链技术项目，但是却没有人致力于建立技术标准，这就是ISO存在的原因。它能够在成员国的努力之下制定标准发展程序，同时还能与其他行业接轨。

（十三）各国对于数字货币不同态度对照

全球多个司法管辖区对于减少虚拟货币的潜在风险，以及监管数字货币相关的活动采取了不同的做法。根据表8.1中所列出监管和政策，

通过各个司法管辖区的不同态度，能够大致看出大家的分歧。

表8.1 各国对数字货币的不同态度

国家	反洗钱/ 反恐：警告 和监管 (现有或建立)	税务处理	对消费 者警告 和建议	数字货币中 介的牌照/ 注册	在金融领 域进行警 告和禁止	禁止 发行 和使用
阿根廷	警告		警告消费者		发布报告 警告	
玻利维亚						是
加拿大	修订现有监管	明确税务处理	建议消费者			
中国					禁止	
法国	使用现有 监管框架	明确税务处理	警告消费者			
德国	使用现有 监管框架					
意大利			警告消费者		警告	
日本	计划建立新的 监管方案		警告消费者	计划建立新的 监管方案		
俄罗斯	使用现有 监管框架		警告消费者			起草 方案
新加坡	计划建立新的 监管方案	明确税务处理	警告消费者			
南非			警告消费者			

国家	反洗钱/ 反恐：警告 和监管 (现有或建立)	税务处理	对消费者警告 和建议	数字货币中 介的牌照/ 注册	在金融领 域进行警 告和禁止	禁止 发行 和使用
英国	使用现有 监管框架	明确税务处理				
美国	使用现有监管 框架（联邦）	明确税务 处理（联邦）	警告消费者	州许可制度 （例如，纽 约州的 BitLicense）		

二、全球证券监管

（一）美国证券交易委员会

2016年4月2日，美国证券交易委员会主席玛丽·乔·怀特（Mary Jo White）发表关于联邦管理机构对于控制区块链的目前和未来计划的讲话。这是2016年来SEC首次公开谈论区块链的潜力，并且明确表态正在研究基于区块链技术的证券发行方式可能会带来的影响。

简单概括就是，在SEC的过去和未来与区块链交易中，怀特号召寻找像区块链这样技术的公司和个人，来加速证券转变。怀特在其公开讲话中谈到，最重要的是在委员会监管制度下区块链的应用程序是否需要注册，如过户代理人或清算代理处。SEC正积极研究这些问题及其影响。

2015年12月16日，SEC批准了Overstock.com的计划，为使用比特币区块链技术的发行证券行提供补助。12月22日，SEC秘书长布伦特·菲尔德（Brent Fields）发表提前声明，发布过户代理人的试行条例，并询问公众对于联邦证券条例下使用区块链技术的想法。

怀特在演讲最后指出，演讲的主题是在急剧变化的金融市场中保护投资者。她担忧新出现的融资渠道对上市之前的创业公司来说并不是好事，新的立法条例目的在于让公司把股权激励作为众筹动力的一部分。包括对于区块链在证券行业潜在影响的评论在内，怀特同样强调了其他“互联网金融的挑战”，包括机器人顾问（或者机器驱动的投资顾问）和市场借贷，用软件直接把借款人和非银行放款人联系在一起。在怀特的演讲中，也谈论了新金融科技“有潜力在任何方面转变市场运作方

式”，这样创新也许对于保护投资者也会有诸多的益处，所以有信心在市场中推动发展。

（二）德国最高证券监管机构

2016年2月，德国顶级证券监管机构——德国联邦金融监管局（BaFin）最新发布的一篇内部刊物文章中，对分布式总账的潜在运用展开研究，包含跨境支付、跨行转账以及贸易数据的存储。虽然对监管细节轻描淡写，但该篇新闻的出炉表明BaFin已看到该技术重塑金融系统中一部分因素功能的可能性，尽管结果可能依然遥远。

2002年5月1日，德国把德意志联邦银行和保险监管、证券监管机构合并，成立统一监管组织——BaFin。BaFin的成立，标志着德国金融监管体系改革的又一次重大变化。联邦金融监管局最高管理层为理事会，由财政部、司法部、内政部和银行、保险公司等机构的人员组成。理事会一年召开三次会议，主要讨论监管局的财务收支问题。联邦金融监管局目前拥有员工1400多名，办公地点分设在波恩和法兰克福，除此之外无任何分支机构。

该机构指出，尽管目前金融业加大甚至全面运用区块链技术的影响尚无定论，但该技术有潜力在金融市场建立一个新标准。BaFin认为承认使用该技术所存在的潜在风险“比以往任何时候都大”，应该继续呼吁全球其他监管机构加强监管。

坚守反洗钱、治理与依从及结算与精算的监管必须得以保障。该机构指出，在这些方面，缺乏中央机构对操作与规范的监管会带来诸多问题。此前，BaFin曾发布有关比特币与数字货币的指导文章，将它们称为“以记账单位为形式的金融工具，却并无法定货币地位”。

（三）国际证监会组织

一个由世界顶级证券交易监管机构组成的组织——国际证监会组织将开始对区块链科技的研究。国际证监会组织也称证券委员会国际组织，是由国际各证券暨期货管理机构所组成的国际合作组织。这个20世纪80年代成立的国际证监会组织致力于加速国际证券监管机构的合作，尤其是信息分享和标准制定方面的合作。中国证监会于1995年加入该组织，成为其正式会员。

在2016年2月16日至18日在马德里举行的IOSCO会议中，区块链技术尤其引起人们的注意。该组织表示，会议讨论研究了如何识别和应对正出现的危机状况。讨论了最近的市场发展状况和世界资本市场的动荡，其实讨论的是互联网金融，尤其分布式网络数据库或区块链带来的挑战和机遇。与会者一致同意对与证券监管有关的金融科技分支机构进行深入研究，其中就包括区块链技术。

证监会秘书长大卫·莱特（David Wright）在2015年12月的采访中，表示区块链技术的透明性给证券监管机构带来了新的机遇。

（四）欧盟最高证券监管机构

欧洲证券及市场管理局（European Securities and Markets Authority, ESMA）是欧盟的最高证券监管机构。ESMA执行董事说，区块链技术可以改进交易后流程。ESMA花了一年多时间，研究比特币等数字货币对欧盟投资环境的影响，并呼吁获取更多技术信息，以便评估其对证券交易周期的影响。

2016年3月初，ESMA执行董事维蕾娜·罗斯（Verena Ross）在英格兰银行和伦敦商学院组织的活动中发表讲话。她指出，尽管相关技术还

处于发展阶段，但ESMA相信分布式总账会广泛应用于交易后环境。ESMA认为区块链技术最可能给这些领域带来好处，包括结算、抵押品管理、所有权记录和证券服务。而实现这个目标需要特殊的参考数据库、所有参与者之间瞬时统一、不可更改的记录共享和透明的实时数据。

当然ESMA也看到这些应用潜在的风险，尤其是在扩展性和安全性方面，以及与现有金融系统之间的互操作性。ESMA尤其关注分布式总账技术大体量操作的能力，管理隐私问题的能力以及保证高安全性的能力。并且，预期逐步采用分布式总账技术，所以它需要展示与其他系统互动的能力。因为这些系统必须与分布式总账共存，比如交易平台。

该董事表示，如果出现垄断的情况，该技术的使用可能引起竞争问题。ESMA相信这可能导致私人区块链系统失去监管透明性。尽管这个系统是为了提高透明度，但是复杂加密技术的使用可能潜在影响透明性和监管。不过，如果区块链技术成功克服了这个障碍，利益将会是非常明显的。比如降低成本、减少去中心化引起的网络犯罪、提高市场整体效率。

不过，该技术的评估还在进行中，ESMA表示会继续研究分布式区块链技术，最终确定是否需要采取监管措施。

（五）澳洲证券投资委员会

澳大利亚最高证券监管机构——澳大利亚证券和投资委员会（Australia Securities and Investments Commission, ASIC）主席格雷格·梅德哥拉夫特（Greg Medcraft）在2016年2月初表示，区块链技术将在政府市场活动监管中产生深远影响。澳大利亚证券投资委员会的基本职能体现在维护市场诚信和保护消费者权益方面。

梅德哥拉夫特从2011年开始任职澳大利亚证券和投资委员会主席。他在2016年2月15日伦敦的一次会议上发表讲话。讲话中，他讨论了资本市场即将面临的数字化技术颠覆性变革，其中特别强调了区块链技术并就监管机构该如何看待和应对这个变革发表了自己的看法。“鉴于变革的速度，我们需要考虑使用那个工具了。”梅德哥拉夫特这样说道。

资本市场运用区块链技术可能提高市场效率，降低交易成本，提高市场透明度，并给希望进入融资市场的投资者和公司提供途径。区块链技术可能会重塑ASIC等监管机构的运作方式，同时提醒注意适当的监管力度。作为对世界监管机构和自己此前讲话的回应。区块链技术对政府监管行为会产生很大的影响。监管机构需要找到监管力度和企业管理之间的平衡点。作为监管机构和政策制定者，需要确保抓住经济更快发展的机遇，而不是阻碍创新和发展。

ASIC希望帮助企业抓住发展机遇，不管是区块链技术还是其他创新科技，其前提都是要保障经济利益。

ASIC主席讲述了澳大利亚证券监管机构的一些应对措施，包括监控公司和产品市场以及区块链监管方法的制定。ASIC正试图找到监控区块链记录的国内外交易的方法。监管机构需要找到恰当的平衡点。

从一系列事件来看，澳洲在区块链上的投入已经远远领先于其他国家，特别是澳洲证券交易所已经投资区块链初创公司DAH超过千万美元，并且正在寻求基于区块链的证券交易解决方案，希望全面升级自己的证券交易系统。而从ASIC的态度来看，他们对于区块链技术持有相当开明的态度，也许能极大地加快区块链技术在澳洲证券交易系统领域和监管领域的发展。

（六）数字货币证券监管框架

在2016年1月，Coin Center发布全球首个《数字货币证券监管框架》。

Coin Center是在美国的数字货币非营利研究和宣传中心，其发布了一份关于对于将数字货币作为证券情况下的报告，提供相应监管的指导框架。本报告的作者彼德·范·瓦尔肯伯（Peter Van Valkenburgh）是Coin Center的研究中心主任。报告提出了一种基于豪威检测（Howey Test）的投资合同框架，以及关于证券管理的基本政策目标。

瓦尔肯伯描述说，Coin Center的工作是发现基于数字货币的几个“关键变量”，并且通过运行和维护相关软件的社区，显示出投资者或者用户的风险。该报告考察了这些变量，并且解释了它们的深度。更进一步映射到豪威检测的“四要素”，来确定数字货币是否类似于一种证券，并因此是否需要被监管。

1946年，美国证券交易委员会在豪威公司（W.J.Howey Co.）一案确立了判定“投资合同”的标准。被告豪威公司是佛罗里达州的一个公司，每年大约种植500亩橘子，将其中一半卖给各地的投资人。豪威公司与投资人签订了土地销售合同和服务合同。联邦最高法院认为，判断证券是否存在，不需要找到正式的股票证书，只要存在有形资产的正式收益，例如对橘园的实际拥有就可以了。同时认为应该放弃形式而注重实质，把判断的焦点放在经济实况上（Economic Reality Test）。

法院提出了一个包括四个要素在内的检验方法，即所谓的“**Howey Test**”：“证券法律中所谓的投资合同是指在一宗合同、交易或计划中，某人（1）利用钱财进行投资；（2）投资于一个普通企业；（3）仅仅由于发起人或第三方的努力；（4）期望使自己获得利润。”将此标准适用于本案，最高法院支持SEC的主张，认为三者构成了《证券法》下定义的“投资合同”进而是“证券”，应按照有关规定登记发行。

在这个案件之后，投资合同被视为确定“证券”定义的灵丹妙药，那

些在“是否属于证券法律管辖”问题上存在争议的交易被原告以“投资合同”的名义诉诸证券法律来解决。根据司法实践，被认定为“投资合同”的，有威士忌酒库存单据、金银投资计划以及会所会籍等。

Coin Center报告主要的观点是，类似于比特币这样的更大、更去中心化的数字货币，被类似于侧链这样的数字货币锚定，以及类似于以太坊这样的分布式计算平台，并不能轻易符合证券的定义，以及并不代表需要通过证券监管来解决会给消费者带来某种风险的可能性。

瓦尔肯伯补充说，可以发现，一些小规模的、比较可疑的，或者某些特定设计的数字货币可能确实是符合证券定义的。本报告的目的是，帮助证券监管者将那些“打着创新名义的骗局”识别出来。报告充满了注释和参考文献，提供了关于数字货币和相关技术的概述，并且对它们的功能、优势和劣势进行了细致的讨论，还分别提供了相关监管指导意见。报告还覆盖了可能会影响用户和投资者风险的变量，以及软件 and 社区的变量，包括透明度、去中心化和开发利益等。

第九章 区块链重塑世界

一、快速变化的开始

全球正在发生快速的变化——包括好的和不好的变化都在快速发生，通过互联网驱动的全球化、社会的期望，以及正在加剧的资源竞争。不同于发展中国家，发达国家和其公民所具有的消费主义倾向和隐私保护，与传统社会价值观以及个人行为准则发生了冲突。这已经不仅仅存在于国家和社区中，负责帮助那些处于困境和艰难时刻的人们。各国政府都在努力满足那些不断增长的消费预期和看似深不见底的社会救助需求。美国前总统肯尼迪曾经发出呼吁“不要问我你的国家能够为你做什么，要问你能为你的国家做什么”——这句话在今天会变得越来越重要：许多公民非常希望能够帮助自己的国家，但在这个数字时代，他们目前还是缺乏社会参与的手段。他们希望成为其中的一部分，而不是一个无助的旁观者。

由于缺乏整个社会参与的手段，将会导致一个结果，即出现两极分化的态度，把不同的期望和看法合并在一起，就会出现把复杂问题简单化的粗暴倾向，从而导致一系列完全割裂的话题的出现。然而，全球的现实是复杂的和混乱的，现实世界、虚拟世界、法律、历史、地理、社会、行为、经济、信息和技术因素交织在一起。而变化还在时刻进行中，不断有新的颠覆性的技术出现，更增加了情况的复杂度。

规模、速度、复杂性都必须综合考虑，这让那些行业领导者、各国政府在理解这种混乱的局面，或是在规划、使用传统的、非协作的组织架构时，变得尤其困难。这特别体现在那些更加灵活的领域，例如在面

对金融市场和有组织犯罪的情形下尤其如此。而越来越多的发展中国家，如肯尼亚和卢旺达，他们没有那么多的包袱，所以可以借助新技术实现跨越式发展。

而在发达国家，一些更小的、更同源的国家正在获得巨大的优势，他们通过提供跨国的国际服务来获利，特别是在欧洲。

这些数字国家的特点包括以下五个方面：

- （1）有数字信息获取能力的领导部门；
- （2）一个足够强大且能够集中力量对全国政府部门进行数字改造的政府，需要具有国际视野，并且能够和所有行业紧密协作；
- （3）一个实时、能协作的国家规划，通过国家投资并且由行业主导；
- （4）每个政府机构需要有对技术了解、合格且经验丰富的政府官员；
- （5）有工程师和IT企业领导经验的政治家。

如果中国希望成为最为先进的数字国家之一，那么在这些领域中，还有许多工作要做。然而世界越来越依赖于数字经济。这就需要在现有的经济模型中使用更多的计算机技术。并且我们必须重新评估我们对于数字经济的理解正在如何变化，以及它的组成部分和相关活动。这就使有些类似从以现金为基础的审计方式转变为以资产为基础的审计方式，不仅需要每个组织有更广阔的视野，能够理解供应链、服务和市场的复杂性，还需要有不同的方式来进行协作方式管理、决策制定、获取分享和责任分担机制。

要在网络空间开展实现数字业务，一个组织必须能够信任和值得被

信任，这都需要让大型和发展的各类社区与其他组织能够进行协作。信任和协作将会是网络空间中最重要因素，远远超过在物理世界中的需求。而区块链在这两方面都能够起到巨大作用，但只取决于人们以何种态度来面对它。

区块链技术的出现并不是来自空中楼阁，其今后发展也不可能脱离互联网和技术原来的脉络，作为一种数据存储机制，其必然也会承接数据结构发展的既定规律。在进行深入分析之后，可以发现这些发展其实从来都是和人类整体思想的发展一脉相承的。随着计算机技术以惊人的速度向前推进，也许我们接近人工智能的奇点也越来越近。有些人拥抱发展，推动发展，也有些人害怕发展，拒绝发展，认为任何的变化都是洪水猛兽，但技术发展的步伐是谁也不能阻止的。我们也许只有遵循这些规律，成为发展的推动者，而不是阻碍者。

二、程序设计理念的变化

比特币哈希算力的存在，意味着它毫无疑问地成了全球最大的算力网络，也意味着即使全球Top（顶级）500的超级计算机的算力加在一起对它来说也可以忽略不计。面对有史以来人类建造的最强大的计算网络，很多传统的系统架构会发生巨大的改变。随着算力的空前发展，“大数据”时代正在向“大计算”时代跨越。

应该说，比特币的计算力加上区块链技术已经处于互联网下一阶段的门槛，所以可以从许多去中心化网络的系统架构上，发现很多设计思路 and 用户需求都已经发生了质的改变，而这些改变可能在未来将对整个IT产生重大而深远的影响。

随着计算能力的充分增加，人们对信息的需求已经不仅是速度快，而是更好、更安全。但是在过去，绝大部分的系统设计都是按照越快实现功能越好的要求来设计的。因为对于过去大多数应用而言，先要实现信息交互的功能才是最重要的。而当人们在互联网上已经有了足够的应用时，就会提出更高的需求。而区块链技术就是顺应这样的要求而出现的。

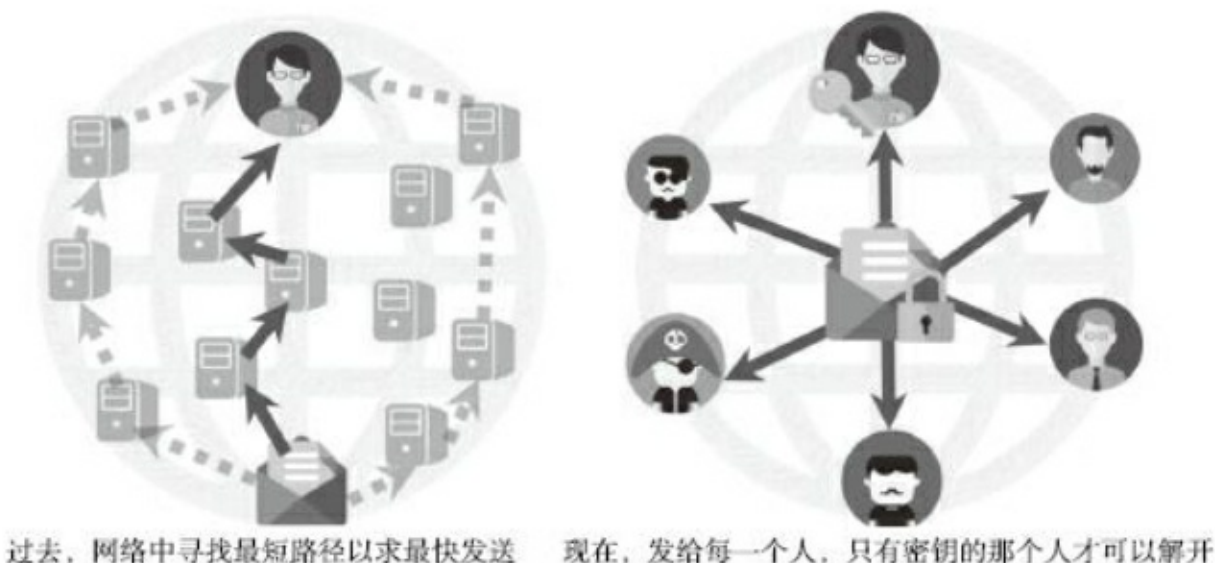


图9.1 过去与现在网络系统架构不同

举一个典型的例子，BitMessage——一个实现类似于电子邮件系统的区块链应用。对于过去传统模型，无论是电子邮件还是其他信息传输系统，总是以快捷为最主要的需求，要求点对点的发送，在点和点之间寻求最短的路径。但是这也很容易让别人追查是谁发给谁，从美国斯诺登事件中披露的信息来看，无论你怎么加密信件内容，其实国安局更感兴趣的是发送给谁，而不一定是内容。

但BitMessage的设计思路 and 传统电子邮件的系统就完全不一样，它在发送一份邮件时，会发送给网络系统中每一个人，每个人都会尝试解密内容，但只有真正有私钥的人才能解开。

这对于过去的软件工程师来说是不可想象的方式，如此浪费计算力和带宽，如此“奢侈”的方式是不是太浪费了？不，因为现在的网络和计算力已经允许这种“浪费”了，因为我们的需求已经从温饱上升至“小康”阶段了。

在充沛的计算力之前，我们愿意并且也能够通过“浪费”一些来换取

更多的安全，这仅仅是一个简单的例子。目前已经有很多试图以区块链技术为基础的应用开始发展，在基于强大安全和算力的基础上开始建立全新的模型，这也许是一个目前还很少有人涉足的金矿。但相信随着区块链技术的发展，会有越来越多和过去截然不同的网络模型和架构出现。

三、数据库进入全新阶段

在互联网诞生初期，数据库主要的类型是关系型数据库，这是一种采用了关系模型来组织数据的数据库。这是在1970年由IBM研究员埃德加·弗兰克·科德（E.F.Codd）博士首先提出的，在之后的几十年中，关系模型的概念得到了充分的发展并逐渐成为主流数据库结构的主流模型。简单来说，关系模型指的就是二维表格模型，而一个关系型数据库就是由二维表及其之间的联系所组成的一个数据组织。

随着互联网Web2.0网站的兴起，传统的关系数据库在应对Web2.0网站，特别是超大规模和高并发的SNS类型的Web2.0纯动态网站已经显得力不从心，暴露了很多难以克服的问题，而NoSQL的数据库则由于其本身的特点得到了非常迅速的发展。NoSQL泛指非关系型的数据库，它的产生就是为了解决大规模数据集合多重数据种类带来的挑战，尤其是大数据应用难题。

以谷歌为例，谷歌公司大数据三篇著名论文（GFS，Bigtable，MapReduce）奠定了谷歌大数据的基础，而谷歌的Pagerank算法实现了当时几乎最先进的数据搜索算法。PageRank通过网络浩瀚的超链接关系来确定一个页面的等级。谷歌把从A页面到B页面的链接解释为A页面给B页面投票，谷歌根据投票来源（甚至来源的来源，即链接到A页面的页面）和投票目标的等级来决定新的等级。简单地说，一个高等级的页面可以使其他低等级页面的等级得到提升。而这个技术正是本章所指的数据第二阶段，通过复杂的设计网络和算法进行重新整理和归纳，将原本看似并无关联的数据变为可以分级分类的高质量数据，让大数据和复杂网络模型成为可能。

但是构建在这之上的大数据，最大的问题就是无法解决信任问题。

因为互联网使得全球之间的互动越来越紧密，与之相伴而来的就是巨大的信任鸿沟。现有的主流数据库技术架构都是私密且中心化的，在这个架构上是永远无法解决价值转移和互信的问题。所以区块链技术将成为下一代数据库架构，通过去中心化技术，将能够在大数据的基础上完成全球互信这个巨大的进步。

区块链技术作为一种特定分布式存取数据技术，通过网络中多个参与计算的节点展开共同参与数据的计算和记录，并且互相验证其信息的有效性（防伪）。从这一点来看，区块链技术也是一种特定的数据库技术。这种数据库将会实现梅兰妮·斯旺（Melanie Swan）所说的第三种数据类型，即能够获得基于全网共识为基础的数据可信性。目前，互联网刚刚进入大数据时代，还处于初期阶段。但是当进入到区块链数据库阶段，将进入到真正的强信任背书的大数据时代。这里面的所有数据都可以获得坚不可摧的质量，任何人都没有能力也没有必要去质疑。



图9.2 区块链数据库的优势

从前面的发展我们可以注意到，数据的发展和马斯洛需求层次理论

有些接近，在实现了生存和使用的需求后，自然会朝着更高的需求进行发展。当然，安全仅仅是数据发展中的一个阶段，而最终会朝着人工智能这个数据自我实现的需求发展。尽管我们还不能确定当数据能够实现人工智能，甚至是数据自我智能时，数据库会是怎样的形态，也许未来的人工智能数据库会变成像电影《复仇者联盟》中的贾维斯和奥创这样的形态吧。

四、金融互联网的出现

我们现在可以展望，这个以区块链技术为基础的全球性支付系统之上，也许将会诞生出一个全新的“金融互联网”。在“金融互联网”中传输的将不是信息，而是资金。这些资金将不仅包括数字货币，也将可以容纳几乎所有各国的法币。而这个网络中，必然是其中使用极低的手续费来让摩擦系数减到最小。

这对于传统金融的冲击将会是巨大的，这在余额宝的发展中已经能够少许了解其中的威力。一个仅仅依靠支付宝系统中的闲散资金来进行的投资基金，一跃成为中国最大的基金公司，彻底改变了中国的基金行业格局。那么如果出现一个全球性支付系统，那中间诞生的商业模式绝对不仅仅会颠覆全球的基金产业了，这其中的破坏性和创造性可能超越所有传统金融人士的想象。

“金融互联网”虽然是依托互联网，但是其一旦成熟，其资金体量可能会远远超越互联网的估值。因为它改变的将会是整个世界中最“昂贵”的部分，它很可能会彻底改变目前的证券、基金、信托、银行和保险等超级巨无霸的模式。任何一个人只要稍微放纵一下自己的想象力就能够领悟到，一个跨越国家法币限制的系统，将会诞生如何空前庞大和全新的证券、基金、信托、银行和保险模式。

金融服务实体经济的最基本功能是融通资金，资金供需双方的匹配（包括融资金额、期限和风险收益匹配）。传统的金融模式可通过两类中介进行：一类是商业银行，对应着间接融资模式；另一类是股票和债券市场，对应着资本市场直接融资模式。这两类融资模式对资源配置和经济增长有重要作用，但交易成本极高，主要包括金融机构的利润、税收和薪酬。

当资产配置全球化的大背景之下，如果能实现全球性支付系统，并且将中间的流通成本降到近乎互联网信息传输的程度，那么作为金融最核心和最本质的作用，融通资金将会获得全新的定义。几乎无缝式的资金对接和资本快速配置会成为所有资本共同追逐的目标，在这个基础上，真正全球意义上的证券、基金、银行和保险都将会诞生。而这将不再是金融寡头们的“自留地”，金融互联网会让这一切变得前所未有的平等和碎片化。就像谷歌重新定义的广告业，余额宝重新定义的基金业。在“金融互联网”的大背景之下，传统的金融模式如果还保持一种抗拒的心态，那么就像邮政业一样，将会被摧枯拉朽般地推倒，成为历史进程中的活化石。

毫无疑问，同互联网一样，“金融互联网”的出现不会由于某些人或某些势力的干预而消失。尽管这对于传统金融体系会造成一系列破坏，就像电子邮件对传统邮政系统的巨大破坏力一样，但是我们相信这其中所孕育的巨大创造力必然会像互联网一样，让我们的社会进入一个全新的阶段。而谁能更早地预见其发展道路和投入其中，也许会成为下一个马云，创造出下一代的阿里巴巴。

我们非常有信心认为我们现在正处在一个重大的转折点之上——和工业革命所带来的深刻变革几乎相同的重大转折的早期阶段。不仅仅是新技术指数级、数字化和组合式的进步与变革，更多的惊喜也许还会出现在我们面前。在未来的24个月里，这个星球所增长的计算机算力和记录的数据将会超过所有历史阶段的总和。在过去的24个月里，这个增值可能已经超过了1000倍。这些数字化的数据信息还在以比摩尔定律更快的速度增长。

我们这一代人将很可能会幸运地经历人类历史上两个最让人吃惊的事件，首先是地球上的所有人和所有机器通过区块链技术以前所未有的互信展开空前的大规模协作，其次就是基于此真正的人工智能将被创造出来。这两个事件将会深深地改变这个世界的经济发展模式。创业者、

企业家、科学家以及各种各样的极客将利用这个充裕的世界去创造能让我们震惊和快乐。

五、资产证券化的加速

Slock.it是一个基于以太坊平台的物联网项目。该项目成员目前主要在德国，希望能够构建一个点对点的智能门锁系统。他们相信在未来所有的门锁都可以通过物联网链接起来，而通过以太坊这样的区块链平台，能够让门禁系统变得具有极高的安全性，并且完全是通过程序和加密算法来自动运作，不依赖任何中心化的机构和管理者进行运营，可以避免任何人为因素造成的损失，也不必担心管理者的道德风险。

该项目目前备受关注，不仅因为它是目前搭建在以太坊上最早的物联网应用之一，并且认为相比其他的区块链项目而言，在目前似乎更容易找到合适的应用场景，此外有一部分投资者认为，该项目很可能会通过物联网，加速全球资产证券化的进程。

Slock.it所打造的智能门锁，让每个人可以用自己的智能设备来进行控制，并且很容易地“制造”出来数量无限的“钥匙”。由于在区块链上能够设计各种复杂的智能合约，从而能够设定复杂的钥匙行为。比如设定任意一把钥匙什么时候可以打开这把锁，也可以设定什么时候不能打开或者直接作废，还可以控制一些更加复杂的行为，比如设定钥匙可以转手的次数，或者是多把钥匙同时在场才能够打开某把门锁。

尽管这种复杂的用途，相比我们目前正在使用的物理钥匙并无太大的实际意义，但其实Slock.it所开发的智能门锁，能够和Airbnb进行完美的结合。

Airbnb是目前全球最大的旅行房屋租赁社区，用户可通过网络或手机应用程序发布、搜索度假房屋租赁信息并完成在线预定程序。Airbnb的用户遍布190个国家近34000个城市，发布的房屋租赁信息达到5万条，被时代周刊称为“住房中的eBay”。

如果有个外国人在网上通过Airbnb进行订房，如果房东的房屋使用了Slock.it提供的智能门锁系统，房东就能够直接通过手机把房屋的“钥匙”通过互联网发送到对方的手机上，并且可以设定该把“钥匙”能够使用的时间段，以及设定当对方租约到期后，“钥匙”就自动作废了。而在传统钥匙的情况下，就很难以这样简便的方式来进行操作。首先无法在网络上把钥匙进行任意的传输，其次很难确保对方不会复制物理钥匙，因此就可能要面对换锁的问题。而通过Slock.it，能够以最便捷和优雅的方式来解决这些问题。

有些人可能会有一些质疑，觉得为什么一定需要在区块链，而不是通过中心化的方式来实现。比如Airbnb为什么不开发这样的系统来进行管理。事实上，类似于Airbnb这样的中心化机构很难开发这样的系统。首先，大多数人并不希望把自己房屋的使用权全部交给一个公司来进行管理，该公司不仅可能需要面临巨大的道德风险，而且如果一旦该机构或者该服务结束，那就可能面临所有用户都要进行大规模的换锁。其次，如果该机构数据库被攻击或者发生大规模的泄露，也很有可能会造成灾难性的后果，而事实上，中心化数据库出现大规模泄露的事件层出不穷。此外，如果所有的租房社区都开发自己的系统就意味着可能要安装多把智能门锁系统，那么这之间的兼容和协调问题对于用户而言也是极为麻烦的。而如果能够有低成本和高安全的方案的话，并且和自己的主营业务并无直接利益冲突的话，即使是中心化机构也不会倾向于自己开发，而是选用已有的公用系统。比如大多数打车软件都不会尝试自己开发地图软件，而是选择现有成熟的技术解决方案。

但对于该项目而言，这仅仅是一切的开始。从某种程度来看，拥有某个房屋的钥匙就意味着拥有该房屋的使用权，那么房东完全可以把钥匙抵押给类似于Airbnb这样的机构，让Airbnb代为出租和管理该房屋，从而获得一定的现金流。考虑到不同房屋的使用价格都不同，抵押不同的房屋钥匙，可能会获得不同金额大小的现金流，因此完全可以把许多不同房屋资产的钥匙进行打包，变成一个资产池（Assets Pool）。并

且，由于在区块链上，几乎所有的数字资产都可以近乎无限分割，因此这些在区块链上的大资产池天生就能够分割为标准化的份额资产，然后在区块链上进行流通。也就是说，这些份额化的资产可以在区块链进行任意的交易、抵押和传输。

在区块链上的所有数字资产可以看作一种凭证，也能够看作是一种有价证券，那整个过程能够视为是一种典型的有资产支持的证券化过程（Asset-Backed Securitization, ABS）。这些房屋在Slock.it的帮助下，很快就能把使用权进行证券化，而且整个过程在区块链上几乎可以自动实现，整个交易过程可以通过基于区块链的去中心化资产交易系统，而无须任何传统资产交易所介入。

显然，智能门锁并不仅仅只安装在房屋上，而是可以安装在任何有门禁系统需要的地方，包括车辆、电脑甚至是洗衣机上。在欧美，很多社区都是集中洗衣的，会有专门的场地放置大量公用投币洗衣机，那么完全可以在这类洗衣机上装上Slock.it这样的智能门锁系统，也就能够把洗衣机进行资产证券化，从而预先获得洗衣机未来的现金流。当然，还有更多的东西可以供我们相信，如果不出意外的话，未来电动汽车将会变得越来越多，所以从现在开始，已经有很多人开始投入巨资建设充电桩，也能够通过装上智能门锁来进行资产证券化。而考虑到份额化交易可以实现近乎无限地分割，也就是说我们能够把充电桩的使用权按秒，甚至是毫秒级进行切分。

所以，从某种意义上来看，Slock.it跨越了物理资产和虚拟资产之间的鸿沟，有潜力将极多的物理资产通过区块链技术实现资产证券化，并且快速实现交易。考虑到这个过程成本很低，而且能够和基于区块链的去中心化交易系统进行完美的解决，也就让整个过程中变得简单和自动化。如果考虑到由于流动性带来的流动性溢价，那么相信一旦Slock.it这样的技术被大众所熟悉之后，会有非常多的物理资产尝试使用它来进行改造和升级，进而让资产证券化变得更加容易和普适。

六、资产发行方式的巨变

面对新技术的崛起，必然有许多相关行业会出现一些巨大的变化。区块链技术的出现可能会使全球金融世界发生很大的变化，特别是资产发行的方式会出现巨大的变化。

目前所有资产发行的方式都是“先审核再发行”，但是区块链技术可能会让整个过程完全逆转，变为“先发行再审核”。也许有人 would 认为，这是无稽之谈，市场监管者肯定不会允许这种情况的发生。但事实是，技术的脚步会摧垮所有的障碍，并且会按照自身的逻辑进行实现。

这种行业的巨大变化并不是第一次。就在20年前，在互联网刚刚开始的时候，整个新闻资讯行业也经历过这个巨大的转变。在很久以前，新闻发布一直是“先审核再发布”，但是互联网技术最终还是让新闻改变为“先发布再审核”，这本身就是互联网对于信息传播的巨大便利性形成的。在没有互联网技术的时候，向许多人进行新闻发布是一件费时费力的事情，所以必然需要通过管控主要的发布通道，才可以很方便地进行审核。即便是在互联网的初期，类似于新浪、网易和搜狐这样的新闻门户网站，也必须有互联网新闻牌照才可以采编和发布新闻。

然而到了今天，每个人拿起手机都能够极其便捷地发布微博和微信。在这种情况下，再进行大规模审核已经变得不太现实，最终会倒逼法律和监管方式的改变，让发布新闻资讯变成“先发布再审核”。

对于资产发布也是如此，现在对于大多数人而言，向全社会发布资产证券化的产品，并且进行交易是有着很高门槛的。但是区块链技术将会让资产发行和交易变得越来越容易，在基于区块链技术的去中心化资产交易平台上，全世界的任何人只要能够接入到网络中，就可以便捷地发布任何资产类型，与他人进行资产交易，完成实时结算和清算。

尽管在这个转变的过程中，可能会出现欺诈、隐瞒或者其他损害他人的情况。但是如果整个市场变得足够透明，某个人希望通过发布虚假资产来欺诈他人会变得非常困难。就像你很难在微博这样的公开社交媒体上欺骗很多人，因为很容易就会被揭穿。而且，也许会出现类似于“浑水公司”这样的团体，通过揭露欺诈行为来获利。

当然，监管者肯定不会喜欢出现这样的局面，他们还是希望将一切都控制在他们能够监控的范围之内。但是技术的发展是无法阻挡的，就像新闻资讯发布一样的，如果有一天发布资产变得和发朋友圈一样简单的时候，最终会倒逼监管和法规顺应技术的脚步。因为无论你喜欢或者不喜欢，技术都可以让更多人做到这一步。

事实上，包括SEC在内的监管机构已经看到了这一点，因此他们在对待Overstock开发的交易系统会做出重大让步，允许他们在去中心化的资产交易平台上进行发行自己的股票，并且进行交易。我们完全可以认为这是SEC已经在测试去中心化交易所的可能性，并且探索区块链技术对证券市场在未来可能产生的影响。

迄今为止，我们还不知道这样的转折点什么时候到来。根据二十多年前新闻资讯发布流程出现改变的时间，这个进程还需要5~10年的时间。但是无论什么时候到来，我们都可以意识到，资产发行流程改变对于现有的证券市场将会产生重大的影响，并且可能会因此完全重构我们目前的金融世界。

七、人类首次大规模协作的开始

对区块链未来前景的看好在于极高的生产力会将这个地球上所有的人人和机器连接到一个全球性的网络中，人类向商品和服务近乎免费的时代加速迈进，也许到了21世纪下半叶，资本主义走向没落，区块链的去中心化协同共享模式将取而代之，成为主导经济生活的新模式。

区块链是这种新兴协同共享模式的最佳技术手段。区块链的基础设施以去中心化的形式配置全球资源，使区块链成为促进社会经济的理想技术框架。区块链的运营逻辑在于能够优化点对点资源、全球协作和在社会中培养并鼓励创造社会资本的敏感程度。建立区块链的各类平台能够最大限度地鼓励协作型文化，这与原始共有模式相得益彰。区块链的这些设计特点带领社会共同走出阴影，赋予它一个高科技平台，将使其有可能成为21世纪决定性的经济模式。

在过去也出现过基于互联网的全球大规模协作科技平台，如SETI@home（搜寻外星文明计划，通过使用志愿者贡献自己的计算机资源来帮助分析来自太空的无线电信号，用于寻找外星文明的迹象）和Folding@home（一个用志愿者贡献的计算机资源来模拟蛋白质折叠的斯坦福大学项目，用于药物计算设计和其他分子动力学问题）这两个已经实施多年的科学项目，但是在过去，这些项目最大的问题是没有一个恰当的奖励回馈机制来鼓舞更多的人参与到这些公益项目中。而区块链机制恰恰是解决这个问题的完美方案。区块链不仅能够提供客观公正的强信用背书服务，而且还能够实现极大规模的高精度奖励回馈机制。

通过奖励回馈机制和智能合约等功能，区块链能够为科学研究提供一个前所未有的全球化协作社区，它将不仅能够把庞大的计算力集合在一起（目前比特币网络所集合的算力已经超过了全球前500位超级计算

机算力总和的一千倍以上），而且能将各种其他所需要的资源进行合理调配和协作，并且通过事先设定好的规则，对参与到整个协作系统中的人、机构甚至是设备进行奖励，来促进资源更加合理地分配，并且吸引更多的资源参与到这个系统中。

区块链让数十亿的人通过点对点的方式接入社交网络，共同创造组成协同共享的诸多经济机会。区块链平台使每个人都成为产消者，使每项活动都变成一种合作。区块链把所有人连接到一个全球性的社区中，将产生前所未有的社会资本繁荣规模，使得全球一体的协作型经济成为可能。没有区块链技术，真正意义上的协作共享既不可行，也无法实现。

由此可以发现，基于互联网的协同合作已经对经济生活产生了深远的影响。市场正让步于网络，所有权正变得没有接入重要，追求个人利益被追求集体利益取代，传统意义上由穷变富的梦想转变成对可持续高质量生活的渴望。也许在不久的将来，现有的社会体系将会失去主导地位，因为全球大规模协作的时代即将到来。

区块链的去中心化特性和高精度奖励模型完全可以深化个人参与协作的程度，该程度和个人在社会经济中协同关系的多样性和强度成正比。这是因为基于通信、能源和物流的各类民主手段使每个个体变得更加强大，但这要求个体有机会参与到这个以区块链技术支撑的去中心化系统中，因此一个通过提高精准回报来增强自主协作精神的时代即将到来。

八、颠覆现代商业社会

我们现在的商业社会大约是在17世纪的欧洲开始逐渐形成的，相对于当时传统的封建社会，这其中有许多对财务制度和法律法规方面的改进。而其中最重要的财务制度和法律法规，莫过于复式记账法、公司制度和保护私有财产的法律。这些制度和规则的诞生，奠定了现代商业社会的基础，从而诞生了一个空前繁华的现代商业社会。因此，我们可以把它们称为商业社会的三大基石。从此，人类社会开始从封建农耕社会开始步入到商业社会，不仅极大地解放了生产力和促进了商业金融的大发展，而且逐步改变了整个人类社会的机构。

我相信，任何一个对于现代商业社会制度熟悉的人，必定会对这三项巨大的创新无比敬仰，因为它们对于推动商业历史的车轮，有着无比巨大的作用。即使到了互联网时代，依旧能够看到它们在推动互联网发展时发挥着良好的功效。然而，区块链有可能将让这三大基石进化到一个全新的阶段。

因为在区块链的世界里，复式记账法变成了分布式总账技术。复式记账法（Double Entry Bookkeeping），是从单式记账法发展起来的一种比较完善的记账方法，也叫复式记账凭证。与单式记账法相比较，其主要特点是：对每项经济业务都以相等的金额在两个或两个以上的相互联系的账户中进行记录（即双重记录，这也是这一记账法被称为“复式”的由来）；各账户之间客观上存在对应关系，对账户记录的结果可以进行试算平衡。复式记账法能够较好地体现资金运动的内在规律，能够全面、系统地反映资金增减变动的来龙去脉及经营成果，并有助于检查账户处理和保证账本记录结果的正确性。而分布式总账技术让系统中每个节点都有机会成为记账人，而每个时间段中都确保账本数据的平衡。其中所有的数据都是可以追溯的，所有的数据不仅具有极高的冗余性，而

且有极高的安全性，完全无法篡改，可以被视为是一种实时审计的记账方式。

公司制度变成了分布式自治公司和组织（DAO和DAC）。不同于传统公司复杂和缓慢的机制，DAO和DAC就像一个完全自动运行的公司，任何一个人都可以随时加入和退出。而公司的股权（代币）成为系统中运行的唯一货币，并让收入、利润这些概念完全消失。公司运作的结构被大大简化，只剩下投资者和生产者，这会极大地提高公司的运作效率。而每一个DAO和DAC，都像上市公司一样，其股权（代币）是可以高速流通的，这意味着其价值发现在一开始就将完全由市场决定的，而不是要通过漫长和复杂的融资和审核方式来逐渐成长为一个上市公司。

而保护私有财产的法律，变成了智能合约。在传统商业世界中，必须通过法律来保障私有财产神圣不可侵犯。而在区块链世界中，这质押依赖于区块链和智能合约就可以做到。在区块链上的资产，及其设定的智能合约是无法被人任意篡改和摧毁的。事实上，区块链中的资产，只要你不交出私钥，就没有任何人能够夺走属于你的资产，也没有人可以改变和终止已经设定好并已经在运行中的智能合约。传统保护私有财产的法律和相关制度是要靠一大堆周边司法设施来保障其运行的，而区块链和智能合约完全靠程序就能实现这样的目的，所节约的社会成本以及提高效率将是传统方式远远不能企及的。

所以，当复式记账法、公司制度和保护私有财产这三个传统商业社会的基石，变为分布式总账技术、分布式自治公司和智能合约，也许会彻底改变现有商业社会的结构和运作方式。尽管区块链技术一直被认为是一种颠覆性的技术，但许多人还是仅仅将其视为一种技术上的变革，但如果我们把视线投向更加深远的社会基础，也许真的能够意识到一场有史以来人类商业社会最大的变革正在拉开帷幕。

区块链社会：解码区块链全球应用与投资案例
龚鸣 著

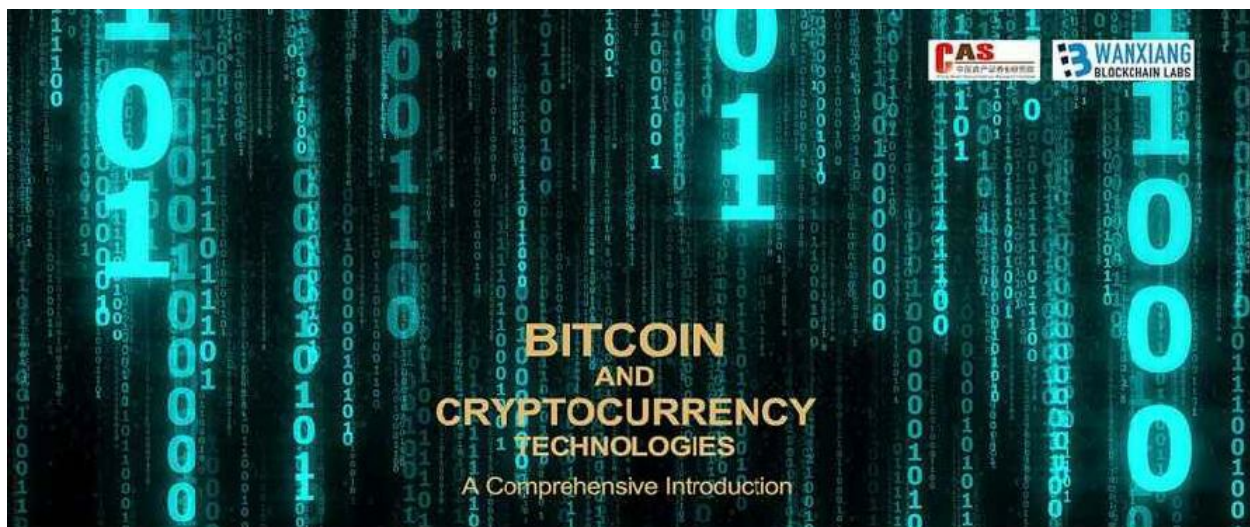
电子书编辑：张畅
版权经理：王文嘉

出 品：中信联合云科技有限公司 www.yuntrust.cn
版 本：电子书
版 次：2016年8月第1版
字 数：300千字

纸书书号：978-7-5086-6444-6
出版发行：中信出版集团股份有限公司 CITIC Publishing Group

版权所有·侵权必究
投稿邮箱：tougao@citicpub.com

中信出版社官网：<http://www.citicpub.com/>
官方微博：<http://weibo.com/citicpub>
更多好书，尽在中信书院
中信书院：App下载地址<https://book.yunpub.cn/>（中信官方数字阅读平台）
微信号：中信书院



区块链 技术驱动金融

数字货币与智能合约技术

[美] 阿尔文德·纳拉亚南 (Arvind Narayanan) 约什·贝努 (Joseph Bonneau)
爱德华·费尔顿 (Edward Felten) 安德鲁·米勒 (Andrew Miller)
史蒂文·戈德费德 (Steven Goldfeder) 著

林华 王勇

帅初 蔡凯龙 许余洁 李耀光 高晓婧 洪浩 译

解密区块链，用技术重构金融世界

谢平 中国投资公司 前副总经理 肖风 中国力向控股有限公司 副董事长 倾情作序

邢早忠 金融时报社 社长

霍学文 北京市金融工作局 局长

刘信义 浦发银行 行长

黄世忠 厦门国家会计学院 院长

唐斌

深圳前海金融资产交易所 联袂推荐
总经理



区块链

——技术驱动金融

[美]阿尔文德·纳拉亚南 约什·贝努
爱德华·费尔顿 安德鲁·米勒 史蒂文·戈德费德 著
林华 王勇 师初 蔡凯龙 许余洁 李耀光 高晓婧 洪浩 译

中信出版社

目录

中文版序 资产证券化可能成为区块链最好的一个应用

中文版序 区块链到底是什么？

译者前言

原版引言

原版前言 通往比特币的漫长道路

第1章 密码学及加密货币概述

1.1 密码学哈希函数

1.2 哈希指针及数据结构

1.3 数字签名

1.4 公钥即身份

1.5 两种简单的加密货币

第2章 比特币如何做到去中心化

2.1 中心化与去中心化

2.2 分布式共识

2.3 使用区块链达成没有身份的共识

2.4 奖励机制与工作量证明

2.5 总结

第3章 比特币的运行机制

- [3.1 比特币的交易](#)
- [3.2 比特币的脚本](#)
- [3.3 比特币脚本的应用](#)
- [3.4 比特币的区块](#)
- [3.5 比特币网络](#)
- [3.6 限制与优化](#)

第4章 如何储存和使用比特币

- [4.1 简单的本地储存](#)
- [4.2 热储存与冷储存](#)
- [4.3 密钥分存和密钥共享](#)
- [4.4 在线钱包和交易所](#)
- [4.5 支付服务](#)
- [4.6 交易费](#)
- [4.7 货币兑换市场](#)

第5章 比特币挖矿

- [5.1 比特币矿工的任务](#)
- [5.2 挖矿所需硬件](#)
- [5.3 能源消耗和生态环保](#)
- [5.4 矿池](#)
- [5.5 挖矿的激励和策略](#)

第6章 比特币和匿名性

- [6.1 匿名的基础知识](#)

6.2 如何对比特币去匿名化

6.3 混币

6.4 分布式混币

6.5 零币和零钞

第7章 社区、政治和监管

7.1 关于比特币的共识

7.2 比特币核心钱包软件

7.3 利益相关者：谁是掌权者

7.4 比特币的起源

7.5 政府对比特币的关注

7.6 反洗钱

7.7 监管

7.8 纽约州比特币牌照

第8章 其他挖矿算法

8.1 算法的基本要求

8.2 反ASIC解谜算法

8.3 有效工作量证明

8.4 不能外包的解谜算法

8.5 权益证明和虚拟挖矿

第9章 比特币“平台”

9.1 比特币作为一个只能被添加的记录

9.2 比特币作为一个“智能资产”

9.3 多方参与的安全博彩系统

9.4 比特币作为一个公共的随机源

9.5 预测市场和真实世界的数据源

第10章 另类币和加密货币生态系统

10.1 另类币的历史和诱因

10.2 几种另类币的详细介绍

10.3 比特币和另类币的关系

10.4 另类币的天折与共同挖矿

10.5 不可分割的交叉链互换

10.6 侧链——基于比特币的另类币

10.7 以太坊和智能合约

第11章 去中心化机构：比特币的未来？

11.1 区块链作为去中心化的工具

11.2 通往区块链融合之路

11.3 去中心化的模板

11.4 什么时候适合去中心化

结束语

术语表

译者简介

中文版序

资产证券化可能成为区块链最好的一个应用

谢平

区块链，这个原本“高冷”的技术词汇，自2015年以来，引起了当前一波又一波最为火热的争议。到底什么是区块链呢？一般人都是因为知道比特币而知道了区块链，也都知道区块链是比特币的一项关键底层技术，通俗些说，它就像是一个数据库账本，安全记录所有的比特币交易信息。按照专家们更为专业的解释来说，该技术的实质是，不同的节点共同参与的分布式数据库，是一个开放式的公共账簿。从数据包形成区块，中间有一个加密的哈希值计算（密码学技术），把不同时间段的交易信息链接起来，就形成了区块链。

信用是金融活动的根基。具体到金融行业，人们正是希望能够通过区块链技术，低成本地解决金融活动中的信任问题。传统金融体系安排中，所有金融活动的监管及中介机构，包括产品登记、证券发行与交易、信息披露、资金托管等方面，都是解决信任问题或者说金融中最为核心的信息不对称问题。由于信任问题是一直难以解决的社会问题，所以，我们这个社会有很多的公信力机构。从反面来说，本次让市场投资者失去信心的长达10年的全球金融危机，全球货币与资产价值的不稳定，就是数字货币和区块链技术被国内外众多金融机构和个人追捧的一个重要背景，区块链技术给我们创造了一个用“共信力”来解决公信力问题的途径。

互联网科技与传统金融机构有待进一步的融合。比如银行业，就需

要更加重视业务经营管理的数字化、智能化建设，更加深入地推广应用移动互联、大数据、云计算、人工智能等先进技术，以科技改造业务、以科技推动创新。正是在这样的思想和认识下，我认为区块链技术也可能为包括银行、保险在内的机构提供当前许多问题的解决方案，不然当前很多以该技术为核心的金融科技公司并没有存在的必要。另一方面，银行家们也明白，区块链不会是银行终结的信号，区块链可以帮助银行和金融机构寻找新的机会，更好地服务客户。

由于对数字货币与区块链有一定的兴趣，希望增加认识 and 了解，我与本书译者林华教授畅谈了上面的认识与体会。这本著作是根据普林斯顿大学公开课改编的一部教材，主要讨论了比特币的一系列重要问题。比如，书中着重介绍了比特币的运作方式、比特币与众不同的技术知识、比特币安全性如何保障、比特币的匿名性特征、区块链如何帮助比特币实现没有身份的共识、人们在比特币这一平台上可以创建哪些应用程序、比特币的存储和使用、比特币挖矿、比特币监管，以及作者们对比特币的未来发展展望。我认为，在阅读完如此专业的教材之后，对当前热议的比特币和区块链的各种争议观点，我们就可以具备去伪存真的能力，或许还能掌握基础概念，并能够开发出安全的、能与比特币网络互动的软件，甚至能够把比特币相关理论应用于自己的项目中。

林教授曾经告诉我，资产证券化与区块链有一个很好的结合点，这是我非常感兴趣的一件事。众所周知，区块链被人们认识主要起源于比特币。比特币的本质是数字货币，区块链的本质在于它是一个分布式账本，而货币系统本身就是一个账本，这是它们能够天然结合在一起的很好解释。只不过，原来的货币系统账本是由央行控制和维护的，现在区块链则是分布式的（也有说成所谓的去中心化），是大家一起共同维护的一个账本。

资产证券化和区块链如何结合呢？一直专长于资产证券化的林教授告诉我说，数字货币的一个延伸在于代币（Token Coin），什么是代币

呢？就是把资产变成货币，代币作为资产使用权的证明，或者资产内在价值的所有权证明。资产变成货币，就是一种证券化。如果我们能够建立一个账本，将资产证券化池子中的资产，全部挪到这个账本上，基础资产的各种特征都做好标记，不断循环，按交易时间更新区块，不可篡改，定期跟踪，就能够实现资产证券化与区块链的一个有效结合。资产挪到账本，还需要从三个层面来说，第一个层面是资产，第三个层面是账本，中间需要一个开关或者说场景，形成一个映射关系，即将资产映射到对应账本上，实现所谓的货币化。中间层需要一个场景，最可能的场景就是交易所，可以实现资产和货币的交易。

当然，我和林华教授都一致认为，这背后还有一个担心，从金融角度来看，区块链在技术上仍然不够成熟，尤其是在交易环节。国内外许多专家都明确估计过，区块链技术可能还需要3~5年时间才能真正成熟。在这样的背景下，如果区块链技术被滥用，就会酝酿很大的风险，就好比前两年的比特币投机潮一样。我认为，如果区块链在交易活动中的跟踪、项目资金使用的全程监控以及智能资产合约所需要的风险控制措施等效用发挥不出来，只是利用分布式的分散管理效果，希望在没有一个第三方公信力机构的情形下保证信用，其结果会很容易搞得像P2P中的债权分拆分包一样，现实中的风险并没有缩小，只是被转移分散到广大投资人中去，最后出现我们看到的P2P机构跑路现象，更要防范的是，现有的P2P都将自己做的债权分拆，包装成所谓的区块链金融。正如北京金融工作局霍学文局长近期所说的，“如果现在不规范区块链技术，它又会成为非法金融活动的来源”。因此，我个人也强烈呼吁，我们要发展的其实是符合金融监管和行业规则的技术创新，如果在区块链技术基础上从事不规范的金融行为的话，也会造成新的非法集资或者金融不稳定的来源。

不过，我依然看好区块链技术在金融领域的运用，它不仅仅是货币创造，而且是价值传输与公共账户。现在国内外很多金融机构在价值传输，比如在支付结算、资产登记以及资产转让等方面也都有积极的探

索。同时，由于区块链是一个公开、透明、可追溯、不可篡改的分布式总账系统，区块链技术可以有效降低支付、清算、结算步骤的出错率，同时监控每一步资金的流入流出情况，是推动诚信社会建立的有效手段，区块链有利于金融监管的一面。随着监管与市场主体对区块链技术的认识不断加深，以及该技术不断走向成熟来保证资产的真实性和林教授一样，我相信资产证券化极有可能成为区块链最好的一个应用。

基于以上的理解和认识，我欣然为林华教授这部翻译作品作序。

谢平

2016年7月

中文版序

区块链到底是什么？

肖风

有关于区块链是什么的话题，在时下的中国，可能已经被包括我自己在内的人说成了陈词滥调了。但是每每我们都会看到这样一种情形：一些我们认为已经是常识的概念，却往往别有洞天！借着《区块链：技术驱动金融》中文版出版之际，我愿意把我最近对区块链概念的反刍心得写下来，作为这本书的推荐序。

区块链首先是一种社会思潮。它预示着人类社会转型、换代的新时代的到来。区块链的社会学基础是凯文·凯利《失控》一书里观察及论述到的基于生物逻辑的自然、社会、技术的进化规律：分布式、去中心；从边缘到中心再到边缘，从失控到控制再到失控。微信之父张小龙奉《失控》为自己行动指南的行为，最好地说明了互联网时代的组织及经济发展规律已经变了。区块链的技术基础是分布式网络架构，正是因为分布式网络技术的成熟，去中心、弱中心、分中心及共享、共识、共担的组织架构、商业架构和社会架构才有可能有效建立起来。本书就是从工程技术的角度来介绍基于分布式网络架构的区块链技术的，分布式网络架构对人类社会的影响和冲击，也许我们都还无法估计，不可测量！

当然，任何事物都是精华与糟粕相生相伴、优点与缺点共存共荣的，区块链技术也一样。在社会实践中我们已经看到，传统金融机构在接受区块链技术的精华的同时，已经扬弃了区块链技术当中的纯粹去中心化的无政府主义色彩和对人人都可以发行货币的去管制、去监管的追

求。

区块链其次是一串技术组合。第一，它是分布式账本：全部机构一本总账、各种事务一本总账；第二，它是新型数据库：没有中心机房，没有运维人员，第三方按共识算法录入数据，非对称加密算法保证数据安全，数据客观可信，不可篡改；第三，它是智能合约：是一段能够自动执行约定条件的计算机程序，依靠智能合约技术，理想中的世界就好像一台精密运行的计算机，一切都可以事先约定，编成代码，依程序行事；第四，它是TCP/IP模型（互联网模型）里的点对点价值传输协议，它的发明标志着过去20几年，互联网技术在帮助人们更好地进行信息传输之后，开始帮助人们可以不借助任何第三方的信任背书，点对点、端到端、P2P地来传递、交易、支付、汇兑价值物。互联网从此进入新时代：价值互联网时代到来了！

区块链还是FinTech（金融科技）的核心。继互联网金融之后，金融科技最近大热大火。我们注意到，前几年互联网金融在中国活跃的时候，欧美国家几乎不为所动。而最近一年，欧美国家反过来把金融科技的火把传输到了中国，在互联网金融一地鸡毛的时候，点燃了中国金融创新的新热点。一开始我也认为，互联网金融和金融科技应该就是一回事。但细细想想，它们之间虽然没有本质不同，却还是重心各有侧偏。互联网金融侧重于场景革命，而金融科技侧重于技术革命；进一步，互联网企业拥有场景优势，所以在互联网金融阶段挟场景的优势，略胜传统金融机构一筹。其实就连互联网公司本身，也有场景能力的高低之分，电商和社交网络公司创建场景的能力最强，所以互联网金融的能力也就最大。其他类型的互联网公司，基本难以望其项背。

而就金融科技而言，侧重的是云计算、大数据、机器学习、人工智能等创新技术。技术是中立的，这意味着：一是技术公司固然有技术先发优势，但金融机构在应用先进技术方面也没有不可逾越的障碍；二是技术逻辑必须与业务逻辑结合才能创造价值，而金融机构在业务逻辑方

面相比技术公司有优势，业务逻辑的经验积累也是需要时间和过程的。无怪乎最近我们看到太多的互联网公司到金融机构挖人的消息，因为在金融科技阶段，互联网公司急需懂得业务逻辑的金融人才。

面对互联网公司的业务竞争，过去几年金融机构的应对举措大概分三类：一是无力回天，沦为通道；二是热情拥抱，全面对接；三是自建场景，创新模式。我们其实在多年以前就已经看到过飞信与微信演绎的故事了，它已经充分说明了切勿以己之短搏人之长的道理。

金融科技有可能是金融机构在与互联网公司业务竞争中的一次最好的机会，因为技术面前人人平等。

所以我们看到，这一次华尔街表现出来的热情超越硅谷。华尔街的金融机构都纷纷表白自己是一家科技公司或马上将成为一家科技公司。

区块链可以算得上是金融科技里的核心技术。因为区块链技术是金融业的底层技术革命。大家知道，现代银行业起源于意大利。之所以起源于意大利，一是意大利是欧洲最早开始海洋贸易的地区，复杂的、高风险的海洋贸易必然需要相配套的金融服务；二是意大利人发明了复式记账法，使得复杂的经济活动在会计上可计量。复式记账法几百年来一直没有重大的改进，区块链技术将是自复式记账法被发明以来，人类社会记账方法的第一次革命性改进。作为分布式账本技术，区块链必将给任何需要记账的行业带来降低成本、提高效率、创新业务、创新服务的机会。金融业因为其早已经数字化的特点，首当其冲，也必先蒙其利！

最后，希望本书的出版，能够从工程技术层面，推动区块链技术在中国的发展，推动相关应用的落地。祝《区块链：技术驱动金融》一纸风行！

肖风

2016年8月

译者前言

这是一本关于比特币和区块链技术的专业著作，起源于业内所熟知的比特币和加密货币技术的普林斯顿网络公开课。以普林斯顿大学计算机科学助理教授阿尔文德·纳拉亚南(Arvind Narayanan)为首的专家，与我们分享了他们关于数字货币与区块链的权威研究成果和重要理论观点。

目前，国内对于比特币和区块链技术的热捧和争议，或者将其过度神秘化，或者将其贬斥得一无是处，还有很多别有用心的人不适当地鼓吹，正是反映出人们并没有真正搞清楚到底什么是比特币，它在技术层面到底是如何运作的。“他山之石，可以攻玉。”本书讨论的是比特币的一系列重要问题。比特币是如何运作的？它因何而与众不同？你的比特币安全吗？比特币用户如何匿名？我们可以在比特币这一平台上创建什么应用程序？加密数字货币可以被监管吗？创建一种新的数字货币将会带来什么样的变化？未来将会如何发展？本书中，作者承认比特币及区块链技术为各种领域带来了颠覆性的创新，但他们并不认可那种以去中心化为目的的观点。

我和王勇教授积极联系与申请，与中信出版社合作，通过激烈的竞争拿到了本书的翻译版权，书中内容的专业性非常强，从翻译初稿到终稿，经过接近一年的辛勤和努力，终于完成了本书的翻译。

在此，我首先要感谢中国投资公司前副总经理谢平先生和中国万向控股有限公司副董事长肖风先生不辞辛苦，亲自提笔为本书作推荐序。感谢金融时报社社长邢早忠先生、北京市金融工作局局长霍学文先生、浦发银行行长刘信义先生、厦门国家会计学院院长黄世忠先生以及深圳

前海金融资产交易所总经理唐斌先生为本书撰写推荐词，感谢您们的鼓励和支持。

我要感谢参与本书翻译的每一位译者。感谢帅初提供了1~9章的翻译初稿，蔡凯龙提供了其余两章和原版前言的翻译初稿。由于本书涉及多个专业领域，翻译初稿在专业性和体例统一等方面有待完善，我组织了所有译者进行重译和修订。其中，高晓婧负责前言与第7章，王勇负责第1章和第2章，洪浩负责第3章和第4章，蔡凯龙负责第5章，许余洁负责第6章和第10章，李耀光负责第8章、第9章和第11章。我、王勇和许余洁确定了全书的术语表，并一同再三审校全书。许余洁在整体校稿的基础上，还多次与出版社老师们对接书稿的最后内容的完善。每一位译者都在工作之余花了很多时间精推细敲、反复斟酌原文和译文，几经修订才使本书得以呈现在读者面前，感谢每一位译者的辛苦付出，也因此我们采用联合署名的译著方式。

另外，我要感谢杨昌丽、黄红华、韩世光、董方朋、王克详等对本书在翻译过程中所提供的帮助。

最后，我还要感谢中信出版社编辑的精心编校，没有大家精益求精的团队努力与合作，这本书的中文版本不可能如此顺利与读者见面。

区块链技术在中国的健康发展，还是要基于我国监管的框架和逻辑下，与适当的行业进行有效结合。我们衷心地祝愿本书的引进，能够有助于大家正确理解比特币金融技术的创新与发展。

林华

2016年7月于北京

原版引言

比特币和加密数字货币是当前的热门话题。乐观主义者认为比特币将从根本上改变人们的支付方式、全球经济甚至政治格局；悲观者则认为它生来就不完美，其失败是注定且彻底的。

究其根本，这些分歧之所以存在，是因为人们没弄清楚到底什么是比特币以及它是如何运作的。本书的目的就是帮助人们跳过噱头切入重点，看清比特币的特殊性。要真正了解比特币的特殊性，我们需要了解它在技术层面的运作模式。比特币是一项新兴技术。把它与现有技术进行简单类比，很难帮助我们做到这一点。

阅读本书需要具备计算机科学的基础知识，了解计算机的工作原理、数据结构和算法，拥有一定的编程经验。如果你是一名计算机专业本科生或研究生、软件工程师、创业者或技术爱好者，那么这本书很适合你。

本书将讨论比特币的一系列重要问题：比特币是如何运作的？它因何而与众不同？你的比特币安全吗？比特币用户如何匿名？我们可以在比特币这一平台上创建什么应用程序？加密数字货币可以被监管吗？创建一种新的数字货币将会带来什么样的变化？未来将会如何发展？

完成本书的学习之后，对比特币和加密数字货币的观点，你应该具备了去伪存真的能力；同时也掌握了基础概念，能够开发出安全的、能与比特币网络互动的软件；还可以把比特币相关理论应用于自己的项目中。

本书网上补充阅读材料中，还包含系列配套练习题，可以帮助

你更深入理解每一章节。此外，你还需要运用到一些要求运用比特币的简化模型，来完成一系列编程任务。本书的大部分内容都有视频，如有需要，可以在免费公开在线课程^[1]上获得(补充材料获取网址为:<http://press.princeton.edu/titles/10908.html>)。同时，建议读者补充比特币相关知识，你可以阅读比特币维基、论坛、研究报告，并与比特币从业者及兴趣相同的人进行讨论。

^[1] Coursera，是免费大型公开在线课程项目，由美国斯坦福大学两名计算机科学教授创办。旨在同世界顶尖大学合作，在线提供免费的网络公开课程。——译者注

原版前言

通往比特币的漫长道路

杰里米·克拉克（Jeremy Clarek）

在通往比特币的道路上，布满了无数失败的尝试。我收集了一份由约100个加密支付系统组成的名单。它们的技术基于电子现金（e-cash）和信用卡，在某些方面获得显著成就，见表0.1。其中一些是被广泛引用的学术研究成果，还有一些是已开发和测试过的实实在在的系统。在这份名单上，被大家所知的大概只有一个——贝宝（PayPal）。而贝宝之所以幸存，得益于它及时纠正了最初想在移动设备上加密支付这一想法。

这段历史会让我们吸取很多教训。比特币的想法从何而来？为什么一些技术成功了而另一些则一败涂地？如何成功地商业化那些复杂的技术创新？即便不去思考这些，它至少让我们明白，一个真实可行的基于互联网的支付体系是多么来之不易。

传统金融体系

设想在政府和货币出现之前，人们以物物交换的方式进行着交易。比如，爱丽丝（Alice）需要工具，鲍勃（Bob）需要药品。如果他们正好都有对方所需物品，就可以进行交换，满足各自所需。

但是，如果爱丽丝有食物，愿意拿食物换工具，鲍勃有工具但不需要食物，他想要药品。在这种情况下，爱丽丝和鲍勃就没法直接与对方

交易。但是，如果有另一个人卡罗尔（Carol），他有药品，而且愿意拿药品换取食物。那么，这三个人就可以进行交易，各自获得所需物品。

表0.1 一些优秀的电子支付系统和构想

ACC	CyberCents	IKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
Checkfree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

当然，难点在于协调，即组织一群供需匹配的人在同一时间、同一地点进行交易。为解决这一难点，出现了两个体系：信用和现金。二者哪个更早出现，历史学家、人类学家和经济学家们就此争论不休，但这对本书的讨论无关紧要。

在上面的例子中，在信用体系里，爱丽丝和鲍勃可以与对方交易。鲍勃给爱丽丝她所需的工具，得到一个人情。换言之，爱丽丝欠下一笔债务，未来终将偿还给鲍勃。爱丽丝的物质需求即刻得到了满足，但她希望尽快还清债务，因此，她又有了新的需求。然后，爱丽丝又遇到了卡罗尔，她可以用自己的食物交换卡罗尔的药品，然后把药品给鲍勃。这样，她就偿还了债务。

对比而言，在现金体系里，爱丽丝可以购买鲍勃的工具，然后把食物卖给卡罗尔，卡罗尔再把药品卖给鲍勃，完成整个闭环交易。只要每场交易的买方有充足的现金，这些交易就可以按任意顺序发生。当然，最终的结果是，看上去现金似乎从未易过手。

很难说这两个体系哪个更优越。现金体系首先需要现金分配来触发，否则交易无法发生。信用体系不需要这样，但债权人需要承担债务人不偿还债务的风险。

现金还可以让我们知道物品的准确价值。物物交换时，我们很难说工具和药品到底哪个更值钱。现金交易把物品的价值标上数字，这就是为什么我们现在将这两种体系混合使用，即便使用信用，我们依然用现金来衡量所需偿还的债务金额。

这些观点被应用于许多场合，特别是用户在进行虚拟物品的线上交易时。例如，在进行点对点（peer-to-peer）的文件分享时，我们就可能遇到吃白食的人，他们只下载，不分享。进行文件交易可能是一个可行的解决方案，但是如何找到两个相互需要对方文件的人是个协调上的难题。在一些项目如莫佐（Mojo Nation）和学术构想如卡玛（Karma）中，用户自动获得一定数额的虚拟货币。接收文件时，用户可以用虚拟货币支付费用；向其他用户发送文件时，赚取虚拟货币。无论是接收还是发送文件，一个或者多个服务器跟踪记录用户的账户余额，而且可以把虚拟货币兑换成真实货币。虽然莫佐项目在推出货币兑换功能之前就消失了，但它算得上是我们现在使用的比特流（BitTorrent，一种内容分发协议）和塔荷（Tahoe-LAFS，一种分布式数据存储方式）的鼻祖。

网络信用卡的弊端

许多电子支付方式都可以根据信用和现金这两个基本概念进行分类。比特币显然属于现金类，但我们先来谈谈信用类。

信用卡交易是目前主要的线上支付方式。如果你在亚马逊这样的网站购过物，那么你应该很清楚流程。首先，输入你的信用卡信息，点击发送，亚马逊收到这些信息后反馈给“系统”，这一系统包括信息处理器、银行、信用卡公司及其他中介。

然而，如果使用贝宝交易，那么你体验的就是中介式结构风格。你和卖家之间存在一个中介公司，你把信用卡信息发送给中介公司，中介公司核准交易并通知卖家，并在每个交易日结束时与卖家统一结算。

这一结构的优势是，你不需要提供给卖家你的信用卡信息，规避了安全风险。你也无须向卖家提供个人信息，保护了个人隐私。劣势在于，它增加了复杂性，你和卖家无法进行直接交流，都得在中介公司开设账户。

如今，我们已经习惯在网络购物时提交个人信用卡信息，至少已经勉强地接受了这一点。我们也习惯了网络公司搜集我们的网络购物及浏览历史。但在20世纪90年代，网络尚是新兴事物，数据加密协议刚刚兴起，消费者对这些问题深感担忧，对网络购物的安全性并不信任。特别是，通过一个不可靠的渠道，把自己的信用卡信息提交给不知名的网络商家，这在当时看来，几乎难以置信。在这种背景下，中介式架构在当时引发了诸多兴趣。

1994年，第一虚拟公司（First Virtue）成立。它是一家较早成立的中介支付公司，也是最早设立完全虚拟化办公室的公司之一。顾名思义，它的员工遍布全国，通过互联网沟通。

第一虚拟公司的支付体系与贝宝现在的体系类似，只是早于后者很多年。用户注册，提交信用卡信息。当用户进行网络购物时，商家把详

细的支付信息发送给第一虚拟公司，第一虚拟公司与用户确认支付信息，确认无误后批准支付。其中有两个细节值得注意：第一，所有沟通都通过电子邮件。那时网页浏览器刚刚开始全面支持HTTPS等加密协议，多方参与增加了加密该支付的复杂性（其他中介采用把信息嵌入URL链接或者在HTTP上定制加密协议的方式）。第二，用户有90天的拒付期，3个月之后卖家才能收到货款。现在，卖家可以立即收到货款，但是消费者依然可以索回货款或者对信用卡账单提出申诉。在这种情况下，商家必须把货款退还给信用卡公司。

20世纪90年代中期，出现了一个较有竞争力的中介体系，我们称之为安全电子交易协议（Secure Electronic Transaction，简称SET）。在SET体系中，用户无须把信用卡信息提供给商家，也无须在中介公司注册账户。进行网络购物时，用户的浏览器会将交易和信用卡信息加密存储在电脑上的应用程序里，只有中介能够解密这些信息，甚至连商家都不能。这样，消费者可以放心地把加密过的信息发给商家。商家再把这些加密信息和它们自己的交易信息一同转发给中介。中介解密你的信息，与商家的交易信息进行对比，只有在双方信息一致的情况下，中介才会批准支付。

SET由维萨（VISA）、万事达以及多家当时重量级的科技公司开发而成，包括网景（Netscape）、IBM、微软、威瑞信（Verisign）和RSA(美国知名信息安全、加密数据公司)。它融合了多个方案，成为一个标准性体系。

一家叫网络现金（CyberCash）的公司采用了SET体系。这家公司在很多方面都很有趣。它们的产品除了处理信用卡支付交易之外，还包括一种叫作网络币（CyberCoin）的数字货币。这是一种小额支付系统，用于支付小额消费行为，比如，用户可以用网络币支付几美分在线阅读报纸的费用。这也就意味着，用户账户里的网络币余额一般都在10美元以内。但是，有趣的是，它们却能得到美国政府联邦存款保险公司

（FDIC）对每个账户高达10万美元的投保金额。

更有趣的是，网络现金公司运行时，美国政府限制加密技术的出口，因为当时加密技术被认为是一种武器。当然，现在这种限制已被废除。但在当时，这也就意味着国外用户无权下载包含加密技术的软件。但是，网络现金公司得到美国政府的特批，国外用户可以下载它的软件。政府给出的解释是，从网络现金公司的软件中提取加密技术远比从头开发一套全新加密技术要难得多。

最后，许多人怀疑网络现金公司与其他为数不多的几家公司一起受到千禧虫感染（Y2K bug），向部分客户重复收费。2001年，网络现金公司破产，其知识产权被威瑞信收购，接着转卖给贝宝，贝宝屹立至今。

为什么SET体系行之有效？根本原因在于它的认证机制。认证就是把加密过的身份，即公钥（public key），与现实身份连接起来。网站要从像威瑞信这样的认证授权公司获得认证，用户的浏览器才会判定它是安全的（通常会显示一个锁形状的图标）。网络现金公司和SET体系认为，安全性比操作的便捷性更重要，因此，它们不仅要求服务商和商家，还要求客户也必须获得认证。获得认证的过程类似于报税一样烦琐，因此，这个系统简直是场灾难。几十年来，大多数用户都拒绝使用要求终端客户认证的系统，这种系统只会出现在学术论文里。比特币巧妙地避开了这一难题，而且无须用户的真实身份。比特币系统通过公钥本身来辨别用户身份。我们将在第1章探讨这个问题。

20世纪90年代中期，正当SET体系标准化时，万维网联盟（World Wide Web Consortium）也在探索如何将金融支付方式标准化。它们试图扩展HTTP协议，这样，用户不需要其他软件，通过浏览器就可以完成交易。事实上，它们对如何扩展HTTP协议提出了一个总体方案，也给出了一个用户支付案例。但这从未付诸实践，整个扩展框架并未应用于浏览器中。近20年后，2015年，联盟宣布重新考虑扩展计划，这次，

比特币将成为该标准化进程的一部分。但是考虑到以往的失败教训，我对此并不乐观。

从信用到（加密）现金

现在该谈谈现金体系了。如前所述，将现金和信用进行比较，我们发现，现金体系需要启动自循环，但优势在于，它规避了买家拒不偿还债务的风险。此外，现金体系还有另外两个优势：第一，更好地确保了用户的匿名性。信用卡与个人信息绑定，因此，银行可以追查消费者的所有消费记录。但是，如果使用现金交易，就与银行无关，卖家也无须知道消费者的个人信息。第二，现金支持线下交易，无须致电第三方获得交易批准。也许交易完成后需要把钱存入银行，但这要容易得多。

比特币没有这两个特点，但具备两个类似的功能。它的匿名性比不上现金。用户在使用比特币支付时，无须使用自己的真实身份，但是，如果用户不够小心谨慎，可以借助公开的交易账目和聪明的算法查出用户的交易记录并最终查出用户身份。我们将在第6章展开这个复杂又有趣的比特币匿名性问题。

比特币并不完全支持线下交易。但优点是，它不需要中央处理器，而是依赖点对点网络，这种网络跟互联网一样具有很强的修复能力。我们将在第3章讨论“绿色地址”和小额支付工具，它们可以帮助我们特定条件和特定情境下进行线下支付。

大卫·乔姆（David Chaum）在1983年最早提出把加密技术运用于现金上的想法。我们可以拿现实中的例子来帮助理解。比如，我向人们发放纸条，上面写着“拿到此条的人可以来我这里领取1美元”。假设人们信任我不会食言而且我的签名不可伪造，他们就可以像银行汇票一样流通纸条。事实上，银行汇票最初就是商业银行发放的支付承诺。只是到

了近代，政府才开始介入，集中货币供给，用法律手段强制要求银行兑现票据。

我可以通过数字签名发放电子纸条，但那样的话，又会遇到一个“双重支付”（double spending）这一恼人的难题：收到表示一定金额的虚拟货币的数据时，人们可以复制该数据，然后传输给他人。假设人们的复制技术足够优秀，我们难以辨别哪些是初始数据，哪些是复制品，那么，我们能够解决“双重支付”的问题吗？

可能的解决方案是：我在发出的每份纸条上印上一串独特的序列号。当别人把纸条给你时，你检查一下我的签名，然后打电话给我，告诉我相应的序列号，询问印有这个序列号的纸条是否已被使用过。如果我告诉你没有，那你就可以放心地收下这个纸条。我会在账本上记录该纸条已被使用。你要做的是定期把收到的纸条交给我，我会再给你相同数量的印有新序列号的纸条。

这个方法是可行的。它在现实中施行起来颇为烦琐，但在网络上却比较简单明了，只要我设置一台服务器，用它来完成签名和序列号的记录工作。唯一的问题在于，因为难以匿名，它很难称得上是真正的现金。不管是发行还是兑现纸条，我都可以把序列号和个人信息一同记录在案。这也就意味着，我能够追踪你的所有消费行为。

乔姆提供了一个创造性解决方案。它不仅能够保护用户的匿名性，同时还杜绝了“双重支付”。它的方法是：我给你一张纸条，你把它的序列号记录下来，并且不要让我看见。然后我再签名，并不需要知道它的序列号。这在密码学里被称为“盲签”（blind signature）。选取一个较长、随机的序列号能够更好地保护你的利益，因为这样的序列号更有可能是独一无二的。我不必担心你选取一个使用过的序列号，因为这样你只会得到一个无效货币而遭受损失。

这是第一个真正意义上的电子货币方案。它虽然有效，但必须要有

一个大家信任的中心机构管理运行的服务器。不仅如此，这个服务器还必须参与每笔交易。如果服务器停止工作，交易就不得不暂停。数年之后的1988年，乔姆与两位密码学专家阿莫斯·菲亚特（Amos Fiat）和摩尼·纳欧尔（Moni Naor）合作，提出线下电子货币的概念。乍看上去这似乎是不可行的：如果用户把同一个电子货币支付给两家没有连入同一个网络或与同一家中心机构合作的不同商家，它们怎么能够发现并阻止这种行为呢？

与其去预防双重支付，不如关注事后当商家重新连上银行服务器的时候如何察觉。这才是比较聪明的做法。乘坐没有网络连接的飞机时，如果你用信用卡消费，真正的转账是在航空公司重新连上网络之后才发生的。如果你的信用卡被拒付，你会欠航空公司（或你的银行）一笔钱。仔细想想，传统金融体系的很大一部分就建立在如何检测错误和损失这一基础之上，然后才是收回损失或惩罚失误方。如果你给某人开一张个人支票，他不会知道这笔钱是否真实存在于你的账户里，但当他去银行兑现时被银行拒绝，他会追究你的责任。类似地，如果线下电子货币系统被广泛应用，国家应该制定相关法律，规定双重支付属于犯罪行为。

为了检测出双重支付，乔姆、菲亚特和纳欧尔三人提出了一种复杂的加密机制。简而言之，这套机制可以达到以下目的：发行方在电子货币中以加密方式嵌入你的个人信息，除了你本人，包括银行在内的任何人都无法解密。你用电子货币消费时，接收方会随机挑选一部分密码要求你解密，并将之记录下来。这种解密的内容不足以暴露你的身份。如果你用同一份电子货币双重支付，当两个接收方都去银行兑现时，银行可以把两份解密的信息合在一起，最终几乎可以肯定知道你的身份。

你可能会担心，万一有人陷害我双重支付呢？比如，你支付给我一份电子货币，我不去银行兑现成有我身份加密的新数字货币，而是直接拿着你给的货币进行重复消费。不必担心，这是行不通的，因为我在用

它支付时，接收方会要求我解密一段密码，这段密码与之前你解密的那段密码肯定是不一样的，因此，我无法完成这一解密任务。

多年以来，许多密码学家一直在研究并完善这一机制。在乔姆、菲亚特和纳欧尔提出的构想中，假设一枚电子货币价值100美元，如果你想买一个价格为75美元的物品，你没法把这枚货币分割成75美元和25美元。你只能去银行，把价值100美元的货币兑换成现金，再拿现金换取价值75美元和25美元的货币。但是，在一篇论文里，Tatsuaki Okamoto和Kazuo Ohta用梅克尔树（Merkle trees）建立了一个可以分割电子货币的系统。梅克尔树在比特币里还会出现，我们将在第1章遇到它。这个机制的效率还有很大的提高空间。特别是，这一机制采用了由史蒂芬·布兰德斯（Stefan Brands）在20世纪90年代，詹·卡姆实（Jan Camenisch）、苏珊·洪博格（Susan Hohenberger）、安娜·莉斯卡亚（Anna Lysyanskaya）在2005提出的“零知识验证”（zero-knowledge proofs），带来了很好的效果。在第6章，我们将看到，零知识验证也同样被运用于比特币体系中。

继续回到乔姆。为把自己的想法商业化，他于1989年创立数字现金公司（DigiCash），应该是第一家致力于解决线上支付问题的公司。数字现金公司比我们之前提过的第一虚拟公司和网络现金公司早了整整5年。数字现金系统使用的现金叫电子现金，另外，它们还有一个名为“网络资金”（cyberbucks）的系统。包括美国的几家银行和芬兰至少一家银行在内的数家银行，确实使用了这个系统。这可是远在比特币出现之前的20世纪90年代，可能会让一些比特币推崇者大吃一惊，因为他们认为银行是惧怕科技、抵制创新的庞然大物。

当你需要交易时，你点击一条由资金接收方发回的链接，跳转至数字现金网页，同时，会开通一条反向链接连回你的电脑。也就是说，你的电脑必须能够接收外部链接，就像一台服务器。你需要拥有自己的IP地址，你的网络服务提供商也必须允许外部连接。如果连接成功，电子

现金软件会在你的电脑上运用，然后你再批准交易，进行付款。

乔姆的数字现金技术获得了几项专利，特别是它使用的盲签技术。外界对他的行为是有争议的，因为专利妨碍了其他人用该技术进一步开发电子现金系统。但是几位经常在一个叫“网络朋克”（cyberpunks）的邮件组里互动的密码学专家则另辟蹊径。著名的中本聪（Satoshi Nakamoto）第一次向全世界宣布比特币系统就是在一个邮件组里，它的前身就是网络朋克，这绝非巧合。我们将在第7章探讨网络朋克运动及比特币的起源。

网络朋克的几位密码学家开发出了一种名叫魔法货币（Magic Money）的类似于电子现金的产品。魔法货币虽然侵犯了电子现金的专利，但因为他们宣称它只用于实验目的，因此并未被禁止。魔法货币是一个很有趣的软件。它采用纯文本界面，你可以通过电子邮件发送交易信息，只需要把交易信息复制粘贴到电子邮件并发送给其他用户就可以了。当然，你需要使用PGP(Pretty Good Privacy，一种加密软件)等终端对终端的电子邮件加密软件，以确保信息在传输过程中的安全。

随后，本·劳里（Ben Laurie）在其他人的帮助下创立Lucre系统。该系统试图用一种非专利技术替代电子现金中的盲签，其他则与电子现金系统大致类似。

另外一个由伊恩·戈德堡（Ian Goldberg）提出的方案则试图解决无法分割电子货币换取零钱的问题。他的思路是：当你没有零钱而向商家支付了过多金额时，如果商家有货币，它会转回给你超额支付的部分。但是应该注意到，这一想法带来匿名性问题。如前所述，在电子现金系统里，付款人匿名而商家不匿名。但是当商家找零时，商家实际上成了付款人，因此他们是匿名的。从你收到商家的找零之后，你需要去银行兑现，这时，你又是不匿名的。这一系统无法确保用户的匿名性，因此，伊恩·戈德堡又重新设立了一个系统，在这个系统中有不同类型的货币，能够确保用户在匿名的情况下既能消费又能收到找零。

为什么数字现金最终失败了呢？主要原因在于它没能说服银行和商家使用它。因为使用这一系统的商家不多，用户也就不愿意用它。更糟的是，它并不或没有支持好用户和用户之间的交易，只侧重于用户和商家之间的交易。因此，商家不接受它，这个系统就很难激发其他人的兴趣。最终，数字现金败给了信用卡公司。

另外，比特币既支持用户和商家之间的交易，也支持用户和用户之间的交易。事实上，比特币体系并不把用户和商家区别开来。比特币的成功很大部分大概要归功于它对用户-用户间交易的支持。从一开始，每位比特币用户都可以发给其他用户，因而整个比特币社区都努力争取人们对比特币的支持，并促使商家也接受它。

数字现金公司的最后几年，它试图通过防侵入硬件来预防双重支付，不再把重心放在双重支付发生后的检测上。在这套系统里，有一种叫作钱包或者类似于卡片的设备。这个设备会记录你的账户余额。消费之后，余额减少；充值之后，余额增加。这个设备的用处是，没有人能够更改计数器数额，不管是通过物理手段还是电子技术。因此，当计数器归零时，倘若没有继续充值，用户都无法消费。

许多公司推出过带有防侵入硬件的电子现金系统。数字现金后来与一家叫CAFE的欧洲公司合作。另一家叫Mondex^[1]的电子钱包公司也是基于这个想法创立的，后来被万事达收购。维萨（Visa）也有类似的系统，名为维萨货币（VisaCash）。

在使用电子钱包时，使用者既持有一张智能卡片，又拥有一个“读卡器”（wallet unit），两者均可进行充值。使用者之间直接可以互相进行支付。支付方将智能卡插入读卡器中，钱即转入读卡器。接受方将卡插入读卡器，钱就转入第二次插入的卡里。这一过程交换的是数字货币，是匿名的交换流程。

Mondex公司在几个地方推广其技术，其中一个城市正好离我的家

乡安大略省圭尔夫市不远。你大概已经猜到，这项技术并没有被广泛使用。主要原因是，电子Mondex卡片跟现金类似，一旦丢失或者被偷，钱也就丢了。更有甚者，如果卡片发生故障，或者读卡器无法读卡，就没法知道卡里余额是多少。这种事情真正发生时，Mondex公司一般会自担损失。它们会假定卡里有余额并赔偿用户损失，这自然是一笔不小的开支。

此外，这个系统里的钱包反应比较慢。用信用卡或现金支付要快得多。商家都不喜欢拥有太多支付终端，对它们来说，一个信用卡POS机就够了。多重原因加在一起导致了Mondex公司的失败。

尽管如此，Mondex公司的用户卡是有小芯片的智能卡片，这项技术事实证明是相当成功的。如今，在很多国家，包括我所在的加拿大，每张信用卡和借记卡都采用了智能卡片技术。它们的目的是防止双重支付。非现金技术中不会存在双重支付的问题，因为银行而不是卡片记录你的账户余额和可用信用。智能卡片的目的是用于认证，也就是说，它为了证明你知道自己账户的PIN。虽然用途不同，早在银行广泛采用该技术之前，Mondex公司就已经开始运用这项技术。

凭空发行货币

如果你有一个价值100美元的电子现金，那怎么能够保证它的确价值100美元呢？数字现金给出的答案很简单：要想获得一个价值100美元的电子现金，你必须从你的银行账户取现100美元，交给发行电子现金的银行。但要实现这个目的可以通过不同的方式，不同的公司采取的方法也各不相同。设想一个小概率事件：如果一个政府授权某家银行发行电子货币，凭空创造新电子现金，会怎么样呢？网格现金（NetCash）就是基于这一假设创立的，但是它并未真正实施过。电子黄金（E-Gold）则采用一套完全不同的体系，它在保险库中存入一定量的黄金，

根据黄金价格发行电子货币。一家名为数字黄金（Digigold）的公司并不完全依赖黄金，但也有部分黄金储备。

归根结底，这些方式都是使电子货币的价值随美元或某种特定商品的价值而浮动。如果美元价值上升或下降，你的电子货币价值就相应地上升或下降。另一种比较激进的方案，就是使电子货币自成体系，其他货币不会影响其发行和价值。

要想创造一种自由浮动并且具有真实价值的虚拟货币，必须要设计出某种具有稀缺性的东西。其实，正是因为黄金和钻石的稀缺性，它们才会成为货币的储备。在虚拟世界，你可以这样设计你的系统，即虚拟货币只有在需要花一段时间解决了一定的数学计算（或“谜题”）之后方可生成，这样就保证了稀缺性。比特币体系中的“挖矿”就是这样的，我们会在第5章详细探讨。

通过解决数学计算来赋予虚拟货币价值，这一想法并不新鲜。早在1992年，密码学家辛提亚·沃克（Cynthia Dwork）和摩尼·纳欧尔（Moni Naor）首次提出这种方案，用来降低垃圾邮件问题。设想你每次发送邮件时，计算机都不得不花几秒钟的时间解决一道数学计算题目。如果你没能附上题目的答案，收件人的邮箱会自动忽略你发来的邮件。对于普通用户，因为他们发送邮件的频率不高，不会带来太大麻烦。但对于想同时发送成千上万垃圾邮件的人来说，解决大量的数学计算几乎是不可能的。1997年，亚当·贝克（Adam Back）在一个名为哈希现金（Hashcash）的体系中采用过类似设计。

要想阻止垃圾邮件，这些数学计算必须具备一定的特性。第一，垃圾邮件发送者解出一道题目之后，不能把这个答案附在他发送的其他邮件上。为了做到这一点，每封邮件会对应一个数学计算题目，题目内容取决于发件人、收件人、邮件内容和发送时间。第二，收件人无须重复解题的烦琐过程，就可以轻松地检查发件人附上的答案。第三，题目之间应是相互独立的，也就是说，解决一道题目不会减少解决其他题目所

需的时间。第四，随着硬件性能的提升，解决数学计算变得越来越快、越来越容易，收件人必须要调整他们收到的答案的难度。通过密码学中的哈希方程（hash functions）设计的题目可以满足以上要求，我们将在第1章学习它。

比特币使用的数学计算与哈希现金的基本类似，只是进行了微小的改进。比特币能做的比哈希现金多得多，毕竟，要解释比特币需要一整本书呢！我之所以提这些，是因为哈希现金的创始人亚当·贝克曾经说过：“比特币只是把哈希现金进行通货膨胀控制得到的延伸产品罢了。”我觉得这话有点过分了，就像说：“特斯拉只是在轮子上加上电池而已。”

正如密码学里任何一个优秀的想法一样，数学计算题目有许多变体，每个变体具有些微不同的特性。其中一个构想来自维莱特（Rivest）和夏马尔（Shamir），他们提出了RSA加密系统（RSA中的R和S分别为Rivest和Shamir的首字母）。研究哈希现金之后我们发现，解决一系列数学计算题目的成本就是解决单个题目的简单叠加。但政府发行货币时，成本可不是这么计算的。单是纸币上的防伪技术，政府就需要投入巨大的初始成本来购买设备，施加安全措施等。但是一旦研发出了防伪技术之后，成本就会降低，印一张货币和印一百张的成本差别并不大。换言之，发行纸币的固定成本很高，但浮动成本很低。维莱特和夏马尔想要设计的数学计算题目具有类似的成本结构，这样，发行第一个电子货币需要巨大的计算量，但接下来就会变得很简单。他们的设计也运用了哈希方程，但使用方式不同。我们打算讨论他们的详细方案，但他们要解决的问题是非常有趣的。

人们为什么没有广泛使用哈希现金来阻止垃圾邮件呢？也许是因为垃圾邮件问题还没有足够严峻。对大多数人来说，垃圾邮件只是个恼人的小问题，并没有严重到他们愿意用计算机算力来解决它。现在，我们有了垃圾邮件过滤器，能够有效地阻挡垃圾邮件。另外一个可能的原因

是，哈希现金无法真正阻止垃圾邮件。特别是，现在大多数垃圾邮件发送人通过僵尸网络，用病毒大量入侵他人电脑，批量发送垃圾邮件。他们也可以通过这些电脑来获取哈希现金。所以，通过数学计算进行限制的想法还在不断发展中。在一些替代网络协议的构想中，如小型LT协议（MinimalLT），我们还可以看到这一思路。

把一切信息都记录在数据库账本中

区块链是比特币的另一项关键技术，它像一个数据库账本，安全记录所有的比特币交易信息。区块链的理论基础由来已久，可以追溯到哈勃（Haber）和斯托尔内塔（Stornetta）在1991年开始发表的一系列论文。他们提出的不是虚拟货币体系，而是一种可以安全地对数字文件进行时间戳记录的方法。时间戳是为了记录文件创建的大概时间。更重要的是，时间戳可以准确反映文件创建的先后顺序：如果一份文件比另一份文件更早创建，可以从时间戳中看出来。时间戳的安全性体现在文件的时间戳一旦生成，无法更改。

用户发送文件时，哈勃和斯托尔内塔设计的体系能够向客户提供时间戳服务。服务器收到文件时，它会用当时时间和指向之前文章的链接或者指针作为签名，来签名该文件并产生包含签名信息的认证，见图0.1。这里所说的指针，指向的不是一个具体地址，而是一串数据。也就是说，如果该数据被更改了，那么这个指针也就自动失效。在第1章，我们将学习如何使用哈希方程来创建这种指针。

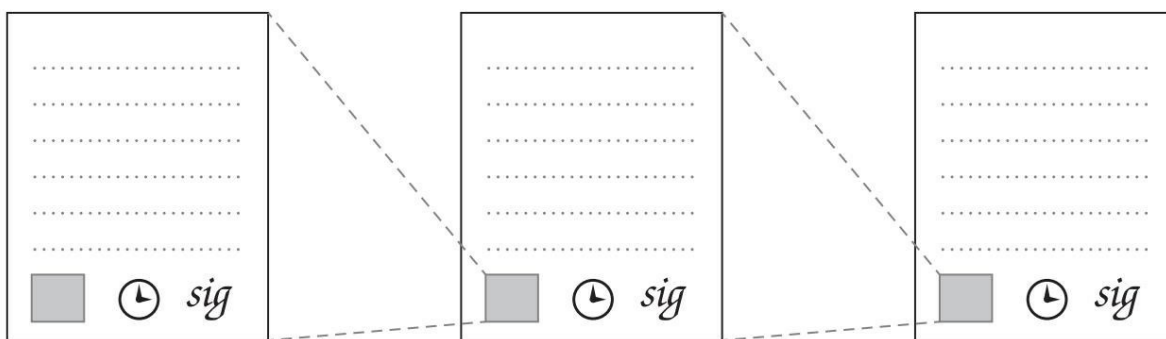


图0.1 链接的时间戳

注：要想对一份文件进行认证，时间戳服务器必须包括指向之前文件认证的哈希指针，当前时间和文件内容本身，并用这三条信息来对文件进行签名。

这种协议实现的效果是：每份文件的认证都确保了上一份文件内容的完整性。其实，反复运用这一理论：每次认证基本上都保障了这个认证点之前的所有文件和认证的完整性。假设这个系统中的每个用户都能记录包括自己的文件、之前和之后的文件的认证在内的几个认证信息，那么合起来，就可以确保整个文件系统不会被更改。特别是，文件的先后顺序被保存了下来。

随后的一篇论文提出了一个可以提升效率的方案：不必单独链接各个文件，而是把它们集合成块，然后在一条链中链接整个块。在每个块里，文件通过树状结构而非线性结构的方式相互链接。这一方法减少了在整个系统中查找特定文件所需的工作量。图0.2展示了这一混合而成的体系的工作方法。

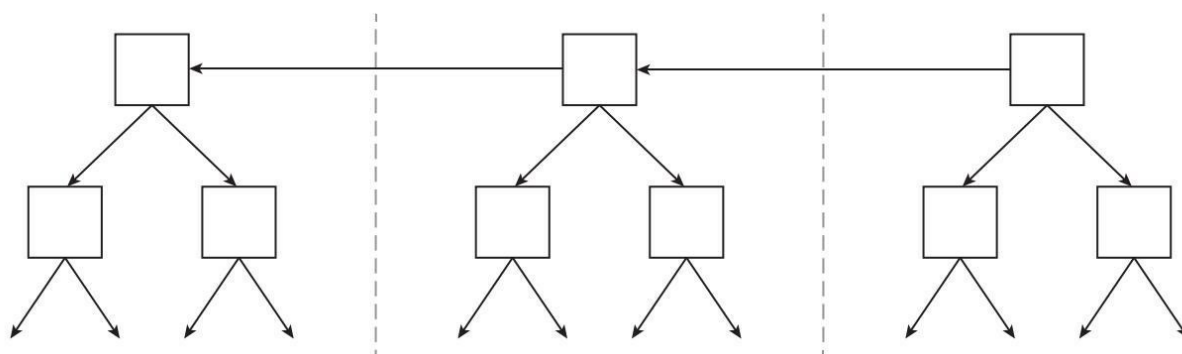


图0.2 高效的链接时间戳

注：箭头表示哈希指针，点状垂直线表示时间间隔。

这一数据结构形成了比特币区块链的框架，我们在第3章可以看到这一点。比特币将它进行了微妙但至关重要的改进，它用一种类似于哈希现金的协议来降低在区块链里增添块的速度。这种改进对比特币的安全性带来了深远而有益的影响。比特币体系通过一群未被认证过的节点，即“矿工”，来记录事件，不再需要认证过的服务器。通过每个矿工而不是普通用户记录块的信息。任何人都可以通过解决数学计算，新建块，而成为一名矿工。比特币还舍弃了签名，只依靠哈希指针来确保数据结构的完整性。最后，真正的时间戳对比特币来说不是很重要，整个系统的意义在于根据先后顺序记录交易信息，并确保它不能被篡改。事实上，比特币块并不按固定时间表产生。在比特币系统里，平均每10分钟产生一个新的块，单相邻的两个块的时间间隔会有较大的差别。

比特币从根本上融合了用数学计算来控制新币的产生和用安全的时间戳来记录交易信息并防止双重支付这两种思路。在比特币之前，有人曾提出过，不这么成熟但也融合了这两种思路的方案。比如，戴伟（Wei Dai）在1998年提出的B币（b-money），任何人都可以通过一个类似于哈希现金的系统创造虚拟货币。它跟比特币类似，也有一个点对点网络。每个节点维护一个数据库账本，但它不同于比特币的区块链，并不记录全部交易信息。每一个节点都有它自认为是准确的记录每个人账户余额的账本。

尼克·萨博（Nick Szabo）还提出一个类似的方案，名为比特黄金（Bitgold）。萨博宣称他早在1998年就有了创建比特黄金的想法，但直到2005年才在博客上公开发布。我之所以提这件事，是因为《纽约时报》记者纳萨尼尔·波普（Nathaniel Popper）曾写过一本关于比特币历史的不错的书，他发现，公开发布比特黄金的那篇博文的发表时间被修改过，改成了中本聪正式发布比特币之后的两个月。他跟许多观察者一样，认为萨博就是中本聪，即使萨博否认。他认为，萨博修改博文发表

时间就是证据，这样，后者就可以掩盖自己在比特币发布之前就已经发明了比特黄金这一事实。

但这一证据并不可信。仔细阅读博文，你就会发现，萨博明确表示自己在1998年就有了比特黄金的想法。他没有试图更改这些时间。更为合理的解释是，比特币开始流行后，他把那篇博文置顶，这样，人们就可以看到他在比特币之前就有了类似的构想。

比特币与B币和比特黄金有很多重要的不同之处。B币和比特黄金通过数学计算直接创造货币。任何人都可以解题，答案本身就是货币。但在比特币体系中，解决数学计算并不构成货币，只是确保区块链安全，间接地在有限时间里创造新货币。此外，B币和比特黄金靠时间戳给货币的创造和转账签名。但比特币不需要被认证过的时间戳，它只是用时间戳来保存区块和交易的先后顺序。

最后，如果服务器和节点对数据库账本的记录不符，B币和比特黄金并没有提供一个明确的解决方案。两位发明人所著文章暗示的解决方案是，由大多数人来决定到底哪个是对的。但是，因为任何人都可以用不同身份设置一个或一百个节点，这个解决方案并不可靠，除非有一个管理员来监管网络入口。比特币则恰恰相反，如果攻击者想更改数据，他必须要比其他所有人加起来的解决数学计算的速度还要快。这样就保证了安全性，还可以让我们量化直观地看到整个系统有多安全。

B币和比特黄金都不是正式发布的体系，B币是在一篇发表在邮件组的文章中提出的，比特黄金则是在几篇博文中提出的。二者未被真正实施和广泛应用。不像比特币白皮书，它们也没有给出详细设定或程序源代码。二者都涉及可能无解的若干问题。其一是前文讨论过的数据库账本不一致的问题。另外的问题是，如何设置创造新货币的数学运算的难度？具有同等运算能力的硬件随着时间的推移越来越便宜，针对这一问题，比特币采用了周期性自动调节运算难度的机制。B币和比特黄金没有这样的机制，因此，它们的货币会因为创造难度降低而贬值。

关于中本聪的猜测

你大概知道，中本聪是比特币创造者的化名。他的真实身份依然是一个谜团，但在比特币早期，他还是比较活跃的。我们可以从他留下的这些印记中，探讨一下他本人，比如说他是从什么时候开始研究比特币的？我们谈论过的那些早期构想对他有什么影响？是什么在激励着他？

中本聪说他从2007年5月左右开始编写比特币。他选择匿名并不表示他会在这件事情上说谎，因此，我姑且相信他所说的。他于2008年8月注册域名bitcoin.org。同时，他开始给一些他认为可能会对比特币感兴趣的人发送邮件，阐述他的想法。2008年10月，他公开发表白皮书，解释比特币协议。此后不久，他又公开了比特币的源代码。随后两年，他在论坛上发布信息，与许多人写邮件交流，回答人们的关切。在编程方面，他对源代码进行了多次修改。他和几位开发人员一同维护源代码，修复补丁。2010年11月，别人逐渐开始接手比特币项目，而他却不再出现。

我用“他”来表示中本聪，但其实我并不知道中本聪到底是男性还是女性，只是因为中本聪是个男性名字而已。此外，我认为中本聪是一个人，而非一个团体。原因是，仔细研究中本聪所有的网络交流记录，在两年的时间里，一个团队里的多个人共用一个账号回复邮件，修改代码，保持风格、语气和内容一致，这简直难以想象。更为合理的解释是，展现在我们面前的中本聪的所有行为是由同一个人完成的。

此外，从他的文章和所打的补丁来看，这个人完全了解比特币的整套代码体系和设计细节。我们有理由相信源代码和白皮书由同一个人所写。最后，可能在一开始有人帮助过中本聪。虽然如此，比特币正式发布之后，我们可以看到，中本聪在得到帮助之后，会很快对其他有贡献的帮助者表示感谢。从这点性格来看，他应该不会在接受别人的帮助之后闭口不言，故意误导人们相信比特币是他一个人的作品。

我们可能会想：“中本聪知道电子现金的历史吗？”为更好地弄清楚这个问题，我们可以看看他在比特币网站上早期发布的白皮书里的引用和索引。在白皮书中，他引用了一些基本密码学和概率论的论文，也引用了我们之前所讨论的时间戳。因为比特币里的区块链与他所引用的内容相似度极高，自然而然地，我们会认为他有参考别人的区块链设计。他还引用了哈希现金，它的数学计算与比特币的非常类似。此外，他还引用了B币。随后，他又在网站上添加了比特黄金和一个由哈尔·芬尼（Hal Finney）设计的重复利用计算数学方案的参考索引。

但是，从与中本聪有早期交流的人公开的邮件来看，我们发现，B币是在亚当·贝克的提议下才加入比特币体系的。随后，中本聪给B币的创造者戴伟发邮件。从邮件中可以看出，是戴伟告诉了他比特黄金。因此，激发中本聪创造比特币的，并不一定是这些方案。他之后与哈尔·芬尼有过多封往来邮件，这可以解释他为什么在网站上或者其他地方引用了芬尼的成果。

基于上述信息，比较可信的推断是，在创建比特币体系时，中本聪只知道电子现金、哈希现金和时间戳，认为只有这些与比特币是相关的。然而，等他知道B币和比特黄金的时候，他才发现，这两个也与比特币有很大关系。2010年，维基百科主编认为比特币不值一提，准备删除比特币词条。中本聪跟另外一些人讨论如何编写比特币词条，好让维基百科接受它。中本聪建议这样描述比特币：“比特币是戴伟在1998年在网络朋克中所提到的B币构想和尼克·萨博提出的比特黄金的具体实现。”可见，中本聪这时确实把比特币看成二者的延伸或具体实施，以便更好地解释比特币的工作原理。

那么，中本聪创建比特币时，他知道其他体系吗？比如我们提过的乔姆的电子现金和信用卡方案。这个很难讲。我们找不到他了解它们的证据，但也有可能他虽然知道，但并未提及它们，因为它们与比特币无关。比特币采用了完全不同的去中心模式，没有理由去提已经失败了的

中心化体系。

中本聪自己也表明了这一点。他在发表在比特币论坛里的一篇文章里，曾粗略地提了一下乔姆的电子现金体系。他当时正在写一篇关于 opencoin.org 的文章，他说他们似乎在“讨论老一套的乔姆中心造币体系，但也许是因为他们别无选择，也许他们会对新的方向感兴趣。20世纪90年代以来所有的虚拟货币公司全都失败了，这导致许多人对这一行业非常不看好。我希望，人们可以看到，这些系统之所以失败，显然是因为它们中心化控制这一特性。我想我们正在首次尝试建立一个去中心化的非认证系统。”从这段话里，我们可以清晰地了解到中本聪是怎么看待之前的系统的，特别是，他认为比特币与它们是不同的。去中心化这一特性确实真正让比特币从其他虚拟货币中脱颖而出。

中本聪写下的另一段话暗示他不是学术派人士。大多数学术研究者先有了构思，然后写下来，再把自己的构思付诸实施。中本聪说他的方式截然相反：“我在建造比特币时，其实是倒着来的。我必须写下所有代码，才能使自己相信我是可以解决任何问题的，然后我才写下理论。我认为我能在写出具体的设计细节之前就可以公开代码。”

中本聪是一个神秘的人，值得一提的是，跟所有人一样，他也会犯错，也无法预测未来。比特币的源代码和设计中都存在很多漏洞和瑕疵。例如，比特币体系有一个可以向IP地址发送比特币的功能。虽然当时人们并未发现，但现在看来，这一设计十分糟糕。中本聪在构建比特币用途时，他主要侧重于比特币在互联网上的使用。这当然是比特币的主要用途，但并非唯一用途。他从未想过，可以去咖啡店用比特币付钱。

了解了虚拟货币的历史之后，我们可能还存在一个疑问：“为什么中本聪要匿名？”有许多可能的原因。首先，也许他就是喜欢这样。许多小说家都选择匿名，像班克西（Banksy）这样的涂鸦艺术家也一直不公开身份。其实，在中本聪活跃的网络朋克社区和密码学邮件组，大家

都普遍采用匿名方式发表文章。

此外，中本聪选择匿名可能还有法律上的顾虑。自由储备（Liberty Reserve）和电子黄金（e-Gold）这两家美国公司都因为非法洗钱惹上了麻烦。2006年，自由储备的创始人之一担心被指控洗钱，逃离美国。电子黄金的创始人一直待在美国，但其中一位创始人被指控洗钱并最后认罪。这一事件正好发生在中本聪创建比特币网站并公开讨论比特币的前夕。纵然如此，许多人都创立过虚拟货币系统，没有人因为法律顾虑而选择匿名。所以很难说这到底是不是他选择匿名的根本原因。

值得注意的是，我们之前提过，电子现金的一些技术是有专利保护的。网络朋克运动担心实施电子现金系统会侵犯这些专利。事实上，有人曾在网络朋克邮件组发表文章，建议由一群匿名的程序员来架设电子现金系统，这样，即使侵权，也查不出是谁。但是，比特币的设计与电子现金的专利差别很大，很难判定比特币侵犯了它的专利权，也许中本聪选择匿名只是比较谨慎。又或者，他是受到网络朋克社区里程序员匿名的启发。

许多人认为中本聪选择匿名是出于个人安全方面的考虑。众所周知，他早期时挖矿获得大量比特币，时至今日，比特币的巨大成功也就给他带来了巨额财富。我认为这个原因是可能的。毕竟，选择匿名不是一时的决定，而是一贯的风格。尽管如此，这可能还不是他一开始就选择匿名的原因。当他首次使用中本聪这个化名时，他还没有发布白皮书和源代码，很难想象他那时就能够预测到比特币后来会取得如此巨大的成功。其实，在早期，中本聪对比特币的未来持乐观且谨慎的态度。他明白许多之前的尝试都失败了，比特币最终也可能失败。

结语

与之前的失败尝试相比，比特币的成功令人瞩目。它有许多优秀的创新，例如区块链和去中心化实现用户之间直接交易的模式等。它能够有效地确保用户的匿名性，虽然还做得不够完美。我们将在第6章详细了解保密性。比特币的保密性从某种意义上来说做得不如数字现金那么好，但从另一个角度来看，它的保密性要更强。因为在数字现金系统，只有消费者能够匿名，商家则不能。比特币为消费者和商家（不管是消费者还是商家）提供了同等程度的保密性。

把比特币和我们之前讨论过的虚拟货币系统进行对比，我学习到的经验教训是：第一，遇到困难时不要轻易放弃。20年来，人们在开发虚拟货币的道路上一直失败，但这并不意味着永远开发不出一套成功的体系。第二，要愿意折中妥协。如果你想把保密性和去中心化功能做到完美和极致，可能就必须牺牲其他的功能。回顾比特币的发展史，它找到了一个完美的平衡点。它的保密性不够完美，需要用户连接到点对点的网络，但用户愿意接受这样的设定。

最后，众志成城。比特币吸引了一批具有激情的用户和开发者，他们愿意为开源技术出一分力，这与之前由公司开发的虚拟货币很不一样，后者的支持者只是公司内部员工而已。比特币如今的成功很大一部分是因为它拥有一个庞大的生机勃勃的支持群体，他们共同推动科技的发展，招徕客户，说服商家采用它。

延伸阅读

一篇关于虚拟货币架构的综述，浅显易懂，侧重实践：

P.Wayner. Digital Cash: Commerce on the Net (2nded).Waltham,MA:
Morgan Kaufmann,1997.

从密码学角度看电子现金系统（第一章）和微支付（第七章）：

B.Rosenberg,ed. Handbook of Financial Cryptography and Security .
Boca Raton,FL: CRC Press,2011.

虽然不是乔姆最早一篇关于电子现金的论文，但这篇是公认的最富有创造性的论文。它的模式成为后来类似论文竞相模仿的对象：

D.Chaum, A.Fiat, and M.Naor.“Untraceable Electronic Cash.” In
CRYPTO 88: Proceedings of the 8th Annual International Cryptology
Conference on Advances in Cryptology .London:

Springer Verlag, 1990.

运用现代密码学技术来提升乔姆-菲亚特-纳欧尔体系效率的论文有许多篇，这是其中最重要的一篇：

J.Camenisch, S.Hohenberger, and A.Lysyanskaya.“Compact E-cash:
Theory and Applications of Cryptographic Techniques,” 2005.

对金融市场和金融构想，包括对Mondex电子钱包体系进行的一些比较实用的安全性分析：

R.Anderson. Security Engineering , second edition.Hoboken, NJ: Wiley,
2008.

乔姆的电子现金构想的实施纲要：

B.Schoenmakers.“Security Aspects of the Ecash Payment System.” In
State of the Art in Applied Cryptography .New York: Springer, 1997.

这两篇论文曾被中本聪在比特币白皮书中引用，被运用于比特币的设计中：

A.Back.“Hashcash—A Denial of Service Counter-Measure,”

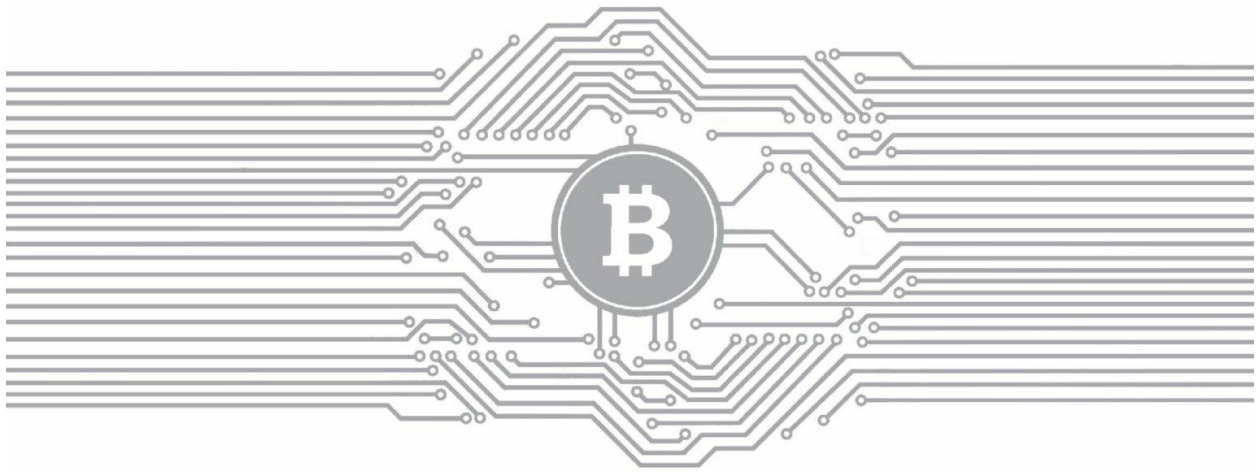
2002.Available at hashcash.org/papers/hashcash.pdf.

S.Haber and W.S.Stornetta.“Secure Names for Bitstrings.” CCS, 1997.

[\[1\]](#) Mondex是一种灵活的电子现金，是当今世界上几种主流的开放式通用电子钱包标准。最初是英国西敏寺银行开发的电子钱包，是世界上最早的电子钱包系统。——译者注。

第1章

密码学及加密货币概述



所有货币都需要通过某种方式控制供给，并需要实施各种安全属性以防止欺骗行为发生。就法定货币而言，中央银行这样的机构控制货币供给，并在实体货币上加上防伪标识，这些安全属性提升了攻击货币的门槛和难度，但并非不可能伪造。最终，执法部门仍需要介入，以防止货币系统规则受到破坏。

加密数字货币也必须采取安全措施，以防御破坏系统状态的行为，同时加密数字货币还需要防止“混淆”，即对不同的人说出相互矛盾的话。例如，如果爱丽丝（Alice）让鲍勃（Bob）确信她向他支付了一个数字币，她就不能再说服卡罗尔（Carol），也给她支付同一个数字币。加密数字货币与法定货币的不同在于，其安全规则需要完全通过技术手段实现，而非依赖于中央机构。

顾名思义，加密货币着力采用密码技术。密码学提供一个将加密货

币体系规则编码到系统本身的机制，我们不但可以利用密码学防止对系统的干扰，并且能够避免混淆，也能用其将新货币单位创造规则编码到数学协议中。为了能够深刻理解加密数字货币系统，我们需要首先探究该系统所依赖的密码学基础。

密码学是一个高深的学术领域，用到了很多不被大众所知的数学理论，并且其理论也比较复杂。幸运的是，比特币只运用到了密码学中少量相对较为浅显的一些理论。在本章中，我们会特别讨论一下密码学中的哈希算法（Hash）和数字签名（digital signature）技术，这两个基本概念对构建一个加密数字货币系统非常关键。在后面的章节中，我们会介绍一些更复杂的密码学理论，例如零知识验证（zero-knowledge proof），这个概念被应用到了对比特币网络的拓展和改进之中。

在学习了必要的密码学基础之后，我们将讨论如何用这些密码学基础构建一个加密数字货币系统。在本章末尾，我们会列举一些简单的加密货币案例，来阐明我们在设计中遇到的挑战。

1.1 密码学哈希函数

我们需要理解的第一个密码学的基础知识是**密码学哈希函数**，**哈希函数**是一个数学函数，具有以下三个特性：

- 其输入可为任意大小的字符串。
- 它产生固定大小的输出。为使本章讨论更具体，我们假设输出值大小为256位，但是，我们的讨论适用于任意规模的输出，只要其足够大。
- 它能进行有效计算，简单来说就是对于特定的输入字符串，在合理时间内，我们可以算出哈希函数的输出。更准确地说，对应 n 位的字符串，其哈希值计算的复杂度为 $O(n)$ 。

这些特性定义了一般哈希函数，以这个函数为基础，我们可以创建数据结构，例如哈希表。我们将只专注于加密的哈希函数，要使哈希函数达到密码安全，我们要求其具有以下三个附加特性：（1）碰撞阻力（collision-resistance）；（2）隐秘性（hiding）；（3）谜题友好（puzzle-friendliness）。

我们会仔细研究这些特性，并会逐步阐释我们为什么需要这样的函数。学习过密码学的读者可能会注意到，我们这里对于哈希函数的论述与一般的密码学课程会有所不同，特别是关于谜题友好。在一般密码学中，谜题友好并非加密的哈希函数的一般要求，却对加密数字货币这一特性非常有用。

特性1：碰撞阻力

加密的哈希函数的第一个特性是它要具有碰撞阻力。这里的碰撞指对于两个不同的输入，产生相同的输出。如果对于哈希函数 $H(\cdot)$ ，没有人能够找到碰撞，我们则称该函数具有碰撞阻力（见图1.1）。即：

碰撞阻力

如果无法找到两个值， x 和 y ， $x \neq y$ ，而 $H(x) = H(y)$ ，则称哈希函数 H 具有碰撞阻力。

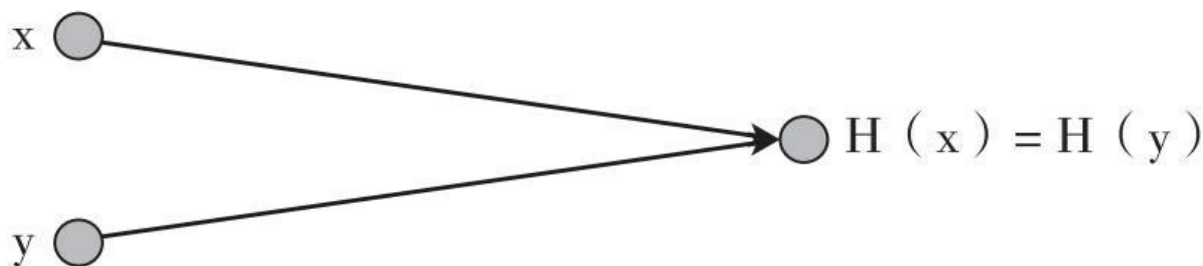


图1.1 哈希碰撞

注： x 和 y 分别是不同输入，当作为哈希函数的输入时，会产生相同的输出。这时我们就说这个函数是哈希碰撞的。

注意，我们说没人能找到碰撞，并不表示不存在碰撞。事实上，通过简单的计数论证（counting argument），我们可以证明碰撞的确存在。哈希函数的输入空间包含所有长度的任意字符串，但输出空间则只包含特定固定长度的字符串。因为输入空间比输出空间大（输入空间是无限的，而输出空间是有限的），一定会有输入字符串映射到相同的输出字符串。实际上，根据鸽巢原理（Pigeonhole Principle），我们可以得出，必然会有大量可能的输入被映射到任意特定输出（见图1.2）。

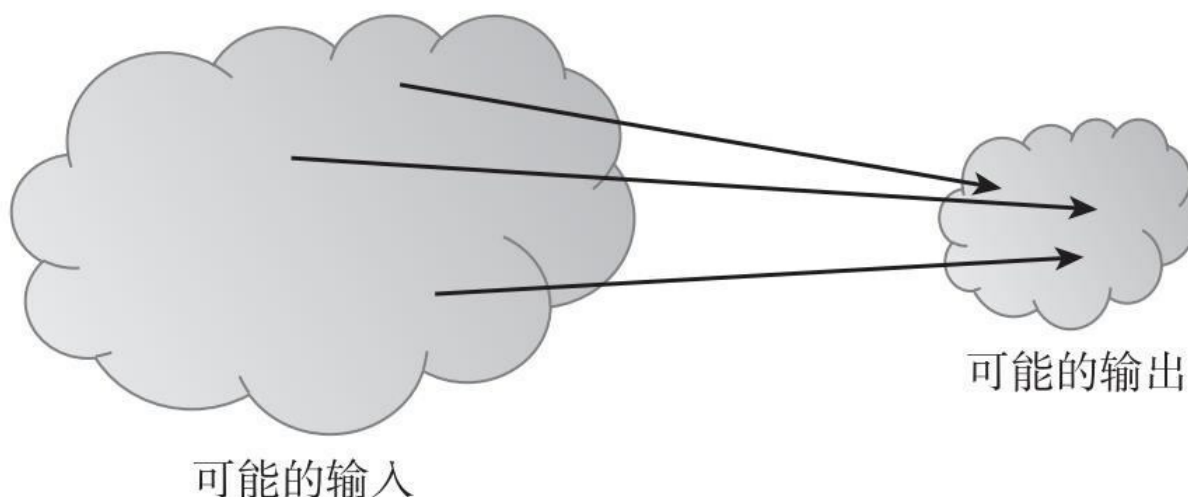


图1.2 必然的碰撞

注：因为输入的数量超过输出的数量，我们可以确定某一个输出肯定对应多个输入。

而更糟糕的是，对于加密的哈希函数，我们虽然说应该找不到碰撞，但有些方法是能保证找到碰撞的。考虑以下对应于一个256位输出大小的哈希函数，选择 $2^{256}+1$ 个不同数值，计算每个数的哈希值，并检查是否有两个相等的输出。因为我们这里选择的输入多于输出，因此在应用哈希函数时，一些数对必将产生碰撞。

使用上述方法一定能找到碰撞。但如果我们随机性地选择输入，并计算哈希值，我们在检验第 $2^{256}+1$ 个输入之前便很可能找到碰撞。实际上，如果我们随机选择 $2^{130}+1$ 个输入值，找到至少两个等同哈希值的概率为99.8%。仅仅通过检验可能输出数量的平方根次数，便大体能找到碰撞，这一事实在概率学中被称为是生日悖论（birthday paradox）[\[1\]](#)。

这个碰撞检测算法对每个哈希函数都有效，但是它的问题是其计算需要花很长很长时间才能完成。对于一个256位输出的哈希函数来说，最坏的情况是你需要进行 $2^{256}+1$ 次哈希函数计算，平均次数为 2^{128} 次，这简直是一个天文数字——如果一台电脑每秒计算10 000个哈希值，计算 2^{128} 个哈希值，需要花 10^{27} 多年时间！换个角度，我们可以说，如果

人类制造的每台电脑在整个宇宙起源时便开始计算，到目前为止，它们找到碰撞的概率仍然无穷小，比下两秒钟地球将被大陨石摧毁的概率还要小得多。

因此，为了寻找一个任意的哈希函数的碰撞，我们只是有了一个一般，但并不实用的算法。一个更艰涩的问题是：有没有其他的方法，可以用于对于某一特定哈希函数找到碰撞？也就是说，虽然一般的碰撞测试算法不适用，但仍可能有其他的算法，可以有效地找到某个哈希函数的碰撞。

以下面的哈希函数为例：

$$H(x)=x \bmod 2^{256}$$

这个函数接受任何长度的输入，产生一个固定大小输出（256位），且能进行有效计算，因此符合我们对哈希函数的要求。但是对于这个函数，我们确实具备一个有效的能够寻找碰撞的方法。注意，这个函数仅返回输入的最后256位，因此，数值3和 $3+2^{256}$ 就构成了碰撞[\[2\]](#)。这个简单的例子表明，虽然我们的一般碰撞测试方法在实践中不可行，但至少对于某些哈希函数，存在有效的测试碰撞的方法。

但对于某些哈希函数，我们无法确认识别碰撞的有效方法是否存在，我们只是怀疑这些函数具有防碰撞特性，但是我们已经证明，世界上没有哈希函数具有防碰撞特性。我们实践中依赖的加密的哈希函数仅仅是人们经过不懈努力之后暂未成功找到碰撞的函数。因此，我们选择相信那些加密的哈希函数具有哈希阻力（在某些情况下，如之前的MD5哈希函数，在多年的努力之后最终找到了碰撞，导致该函数在实践中被逐渐淘汰，最终被弃用）。

应用：信息摘要

现在我们知道什么是碰撞阻力了，我们自然会问：碰撞阻力有什么用途？以下就是一个应用：哈希函数**H具有碰撞阻力**， x 和 y 是两个不同的输入，那么可以假设它们的哈希函数 $H(x)$ 和 $H(y)$ 也不同——如果已知 x 和 y 不同，但哈希值相同，那么H具有碰撞阻力的假设就不成立了。

这个论证使我们可以将哈希输出作为**信息摘要**（message digest）。以SecureBox为例，SecureBox是一个允许用户上传文件，并保证文件被完整下载的线上文件存储系统。假设爱丽丝上传了很大的文件，并希望能够在之后下载时确认她下载的文件与她上传的文件相同。一种方法是将整个文件进行本地存储，并直接将其与下载文件对比。如果这样可行，那么将文件上传便显得毫无意义，倘若爱丽丝需要使用本地文件副本以保证其完整性，她可以直接使用本地副本。

无碰撞哈希函数为这个问题提供了简单有效的解决方法，爱丽丝只需要记住原文件的哈希值，从SecureBox下载文件后，她可以计算下载文件的哈希值，并与原文件哈希值进行对比。如果哈希值相同，那么爱丽丝可以说该文件就是她上传的那一个，但是如果不同，她则可以确定文件被破坏了。记录哈希值可以帮助爱丽丝检测文件在传输过程中，或在SecureBox服务器上是否产生了意外损坏，或者检测文件是否受到服务器的蓄意修改。保证主体不受其他实体的恶意行为侵害，这正是密码学的核心。

这里的哈希函数对于一个信息生成固定长度的摘要，或生成了简明总结，这为我们提供了一种记住之前所见事物，并在今后认出这些事物的有效方法。虽然整个文件可能非常大，存储规模达数G，但其哈希值的长度固定。例如，哈希函数为256位。这样做，极大地降低了存储要求。在本章后面及整本书中，我们都会看到哈希作为信息摘要的应用。

特性2：隐秘性

我们希望哈希函数拥有的第二个特性是其**隐秘性**。隐秘性保证，如果我们仅仅知道哈希函数的输出 $y=H(x)$ ，我们没有可行的办法算出输入值 x 。问题是，上述的表示形式不一定是正确的。考虑以下简单的例子：我们做一个抛硬币的实验，如果抛硬币结果为正面，我们会宣布字符串哈希为“正面”；如果结果为反面，我们会宣布字符串哈希为“反面”。

然后我们问我们的对手，在他没有见到抛硬币，而只见到哈希函数的输出的前提下说出哈希函数的输入字符串（很快我们就知道为什么要玩这个游戏了）。为了回答问题，对手会简单计算“正面”字符串的哈希值及“反面”字符串的哈希值，然后对手便可以知道他得到的是哪一个。这样，只需要几步，对手就能反解出输入值。

对手能够猜出字符串，这是因为 x 只有两个可能，他可以很轻易地将两个可能对应的哈希值计算出来。为了实现隐秘性，我们需要 x 的取值来自一个非常广泛的集合，也就是说，仅仅通过尝试几个特定的 x ，就能找到输出值的方式将不会发生了。

现在的问题是：在类似抛硬币的“正面”、“反面”实验中，如果我们想要的反解的输入值并非来自分散的集合，我们是否还能得到隐秘性？幸运的是，对于这个问题答案是肯定的！我们甚至能够通过另一个较为分散的输入进行结合，而将一个并不分散的输入进行隐秘。现在我们可以更精确地表示隐秘的含义了（双竖线 \parallel 为连接符号，代表把一系列事件、事情等联系起来）。

隐秘性 哈希函数 H 具有隐秘性，如果：当其输入 r 选自一个高阶最小熵（high min-entropy）的概率分布，在给定 $H(r \parallel x)$ 条件下来确定 x 是不可行的。

在信息论中，**最小熵**是用于测试结果可预测性的手段，而高阶最小熵这个概念比较直观描述了分布（如随机变量）的分散程度。具体来说，在从这样分布中取样时，我们将无法判定取样的倾向。举个具体的例子，如果 r 是从长度为256位的字符串中随意选出的，那么任意特定字符串被选中的概率为 $1/2^{256}$ ，这是一个小到几乎可以忽略的取值。

应用：承诺

现在来看一下隐秘性的应用。具体来说，我们把想做的事情称为**承诺**（commitment）。这里承诺是一个数字化过程，可以类比为以下动作：首先选定一个数字，将数字装进信封，然后将该信封放到一个人都看得到的桌子上。这样做以后，可以说你就信封里的数字做出了承诺，在打开信封前，虽然你已经做出了承诺，对其他人来说它还是秘密。在之后，你可以打开信封，来展示承诺的数值。

承诺协议 一个承诺协议方案由两个算法构成：

- $\text{com} := \text{commit}(\text{msg}, \text{nonce})$ ，承诺函数将信息（msg）和一个临时随机数（nonce）作为输入，输出就是一个“承诺”。

- $\text{verify}(\text{com}, \text{msg}, \text{nonce})$ ，验证函数将某个承诺输出（com）、临时随机数（nonce）及信息（msg）作为输入，如果 $\text{com} == \text{commit}(\text{msg}, \text{nonce})$ ，则返回“真”（true）；反之则返回“假”（false）。

我们要求以下两个安全特性要成立：

- 隐秘性：已知com，没有可行的方法找到msg。
- 约束性：没有可行的办法找到两组 $(\text{msg}, \text{nonce})$ 和 $(\text{msg}', \text{nonce}')$ ， $\text{msg} \neq \text{msg}'$ ，而 $\text{commit}(\text{msg}, \text{nonce}) == \text{commit}(\text{msg}', \text{nonce}')$ 。

| nonce')。

为了使用承诺方案，我们首先需要产生一个临时随机数。然后将这个临时随机数与承诺信息msg一起代入承诺函数，计算承诺函数输出值com，然后公布该输出。这个过程就如同将封好的信封放到一个人人能看到的桌上那样。之后，如果我们希望展示之前的承诺值，我们首先公布用于产生承诺的临时随机数，并公布信息msg。此时任何人都可以验证这时公布的msg是否为之前承诺，这个阶段就如同打开信封。

| 对于每次的承诺值，你都需要选择新的随机值，这一点很重要。在密码学中，术语nonce是指，该取值只能使用一次。

以上两个安全特性决定了这一算法就如同密封及打开信封。第一，如果仅仅知道com，即承诺函数的输出，就如同只看信封并不能得到信息内容；第二就是约束性，这就保证了你一旦承诺信封内的内容，就不能再改变主意。也就是说，我们无法找到两个不同的信息，当你在承诺一个信息后，而又声称你承诺了另一个信息。

我们如何在承诺协议中保证隐秘性和约束性这两个性质成立呢？在讨论这一点之前，我们需要讨论如何执行承诺方案。我们可以通过使用加密的哈希函数来达到目的，考虑如下承诺协议实施方案：

$$\text{commit}(\text{msg}, \text{nonce}) := H(\text{nonce} \parallel \text{msg})$$

其中，nonce为长度为256位的临时随机数。

为承诺一段消息，我们首先生成一个256位的临时随机数，然后将这个临时随机数与信息链接，并返回这个链接值的哈希值，来作为承诺输出。为了便于验证，我们还要设定其他人来计算一下临时随机数与信息链接之后的哈希值，比对一下计算结果是否与承诺输出相同。

再来看一下我们的承诺方案要求的两个特性，如果我们将承诺和验证换成 $H(\text{nonce} \parallel \text{msg})$ ，那么这些特性就变成：

- 隐秘性：已知 $H(\text{nonce} \parallel \text{msg})$ ，没有可行方法找到 msg 。
- 约束性：没有可行方法找到两对 $(\text{msg}, \text{nonce})$ 和 $(\text{msg}', \text{nonce}')$ ， $\text{msg} \neq \text{msg}'$ ，而 $H(\text{nonce} \parallel \text{msg}) = H(\text{nonce}' \parallel \text{msg}')$ 。

承诺的隐秘特性正是我们要求哈希函数要具备的隐秘性，如果将一个解密密钥选定为256位的随机值，那么由隐秘性得出，如果解密密钥与信息链接，那么仅仅从哈希函数的输出中恢复信息就是不可行的。约束性隐含在哈希函数的碰撞阻力特性中[\[3\]](#)，如果哈希函数具有碰撞阻力，那么我们将不能找到不同的 msg 及 msg' 值，而 $H(\text{nonce} \parallel \text{msg}) = H(\text{nonce}' \parallel \text{msg}')$ ，如果这种情况发生，将构成碰撞。

因此，如果哈希函数 H 具有碰撞阻力及隐秘性，从安全特性上来讲，这个承诺方案将有效。

特性3：谜题友好

哈希函数需要的第三个安全特性为谜题友好特性。这一特性较为复杂，我们首先解释该特性的技术要求，然后通过举例来阐释该特性的意义。

直觉上，谜题友好可以这样解释，如果有一个人想找到 y 值所对应的输入，假定在输入集合中，有一部分是非常随机的，那么他将非常难以求得 y 值对应的输入。

谜题友好 如果对于任意 n 位输出值 y ，假定 k 选自高阶最小熵

分布，如果无法找到一个可行的方法，在比 2^n 小很多时间内找到 x ，保证 $H(k \parallel x) = y$ 成立，那么我们称哈希函数 H 为谜题友好。

应用：搜索谜题

现在，让我们试想一个应用以阐释谜题友好特性的意义。在这个应用中，我们将建立一个搜索谜题，该谜题是一个需要对庞大空间进行搜索，才能找到解决办法的数学问题。该搜索谜题没有捷径，也就是说除了搜索庞大的空间来进行求解，别无他法。

搜索谜题 搜索谜题构成：

- 一个哈希函数 H 。
- 从高阶最小熵分布选出的一个取值， id （我们称其为谜题ID）。
- 目标集合 Y 。

该谜题的解决方法为一个解， x ，应该满足以下公式：

$$H(id \parallel x) \in Y$$

这个直觉是：如果 H 有一个 n 位输出，那么它的可能取值有 2^n 个。解决这个谜题要求找到一个位于集合 Y （通常比所有输出值集合小很多）内的输出值， Y 的大小决定了谜题的难度。如果 Y 是所有 n 位字符串的集合，这个谜题就毫无意义。然而，如果 Y 只有一个元素，那么这个谜题难度最大，谜题ID取自高阶最小熵分布，这个事实保证了求解无捷径。反过来，如果该ID的确定性很高，那么有人可能会作弊，比如通过使用该ID，事先对谜题进行求解。

如果一个哈希函数具备谜题友好特性，这就意味着对于这个谜题没有一个解决策略，比只是随机地尝试x取值会更好。因此，如果我们要把谜题做成很难解决是可以的，只要我们能采用适合的随机方式生成谜题ID。当我们讨论比特币采矿（是一种搜索谜题）时会采用这一思路。

安全哈希算法

我们讨论了哈希函数的三个特性及其相应的应用。现在，让我们讨论本书中将会大量用到的一个哈希函数，**安全哈希算法**（Secure Hash Algorithm 256，简称SHA-256）。哈希函数有很多，但SHA-256是一个主要被比特币世界采用，并且效果还很不错的哈希函数。

回想一下，我们要求哈希函数可以用于任意长度输入。幸运的是，只要我们能建立一个用于固定长度输入的哈希函数，然后通过一般方法，就可以将接受固定长度的哈希函数转化为可接受任意长度输入的哈希函数，我们称这个转换过程为**MD**（Merkle-Damgard）**变换**，SHA-256是采用这种变换方法的常用哈希函数之一。在通用术语中，这种基础型，可用于固定长度，具备碰撞阻力的哈希函数被称为是**压缩函数**（compression function）。经过验证，如果基本压缩函数具有碰撞阻力的特性，那么经过转换而生成的哈希函数也具有碰撞阻力。

MD变换很简单。比如压缩函数代入长度为m的输入值，并产生长度短一些为n的输出值。哈希函数的输入（可为任意大小）被分为长度为m-n的区块。MD变换运作过程如下：将每个区块与之前区块的输出一起代入压缩函数，注意，输入长度则变为 $(m-n)+n=m$ ，也刚好就是压缩函数的输入长度。对于第一个区块而言，之前没有的区块，我们需要选取一个初始向量（见图1.3）。每次调用哈希函数，这个数字都会被再一次使用，而在实践中，你可以直接在标准文档中找到它。最后一个

区块的输出也就是你返回的结果。

SHA-256函数利用了这样的一个压缩函数，这个压缩函数把一个768位的输入压缩成一个256位的输出，每一个区块的大小是512位。我们可以通过图1.3来理解SHA-256的工作过程。

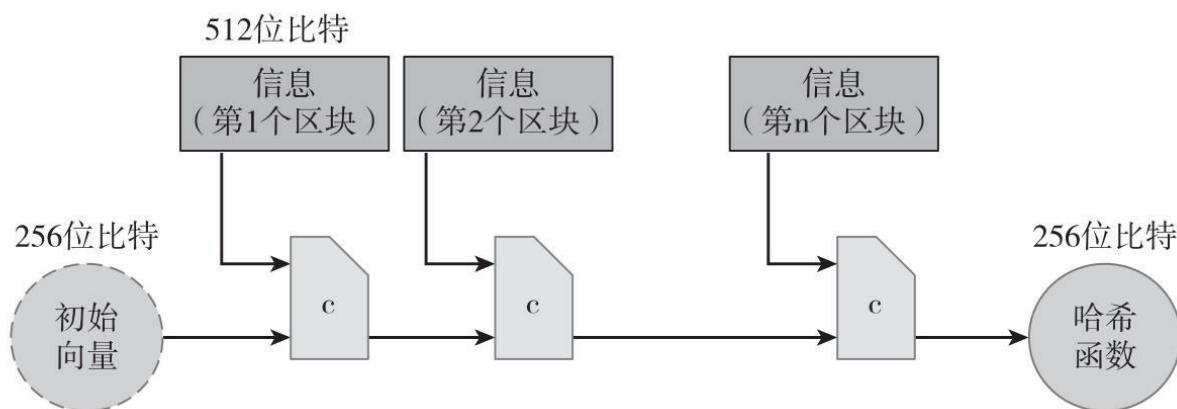


图1.3 SHA-256哈希函数简化图

注：SHA-256利用MD变换把一个固定输入的防止碰撞的压缩函数变换成一个接受任意长度输入的哈希函数。通过初始化向量的补位，可以把输入变成512位比特的整数倍。

截至目前，我们已经讨论了哈希函数、密码学上使用具备特性的哈希函数、这些特性的应用，以及在比特币世界中使用的一类特殊的哈希函数。在下面的章节中，我们将讨论通过哈希函数来构建比特币网络中的更为复杂的数据结构。



哈希函数建模

哈希函数是密码学中的瑞士军刀：它们在众多各具特色的应用中找到了一席之地。这种多功能性的另一面是，为了保证安全，不同的应用会要求不同的哈希函数特性。事实已经证明，要确定一系列哈希函数特性以全面达成可证安全极度困难。

本书中，我们会选出在比特币和其他加密数字货币中，对哈希函数使用方式很重要的三个特性。即使在这个范围内，并非所有这些特性对哈希函数的每一次使用都有必要。比如，我们之后会看到，谜题友好只在比特币采矿中具有重要性。

安全系统设计师常常会放弃，并且把哈希函数建立成对于任意一个可能的输入，都会得到一个独立的随机输出的函数。这种使用“随机预言模式”来证明安全的做法在密码学中仍具争议。不论在这个辩论中你的立场如何，在建立安全系统时，当我们应用哈希函数基本特性，推论如何减少安全特性的数量，都是宝贵的智力训练。本章的目的便是帮你学习这一项技能。

[1] 生日悖论是指，如果一个房间里有23个或23个以上的人，那么至少有两个人的生日相同的概率要大于50%。这就意味着在一个典型的标准小学班级（30人）中，存在两人生日相同的可能性更高。对于60或者更多的人，这种概率要大于99%。——译者注

[2] 3 和 $3+2^{256}$ 对 2^{256} 求余数之后，结果都是 3 。——译者注

[3] 结论反之不成立，就是说，我们可以找到碰撞，但都不是满足 $H(\text{nonce}\parallel\text{msg})==H(\text{nonce}\parallel\text{msg}')$ 意义下的碰撞。例如，你可以对于同一个信息来产生满足同一承诺的随机数，但这里的哈希函数不具备碰撞阻力特性。

1.2 哈希指针及数据结构

本节将讨论哈希指针（hash pointer）及其应用。哈希指针是一种数据结构，这种数据结构在我们即将讨论的很多系统中都很有用。简单来说，哈希指针是一个指向数据存储位置及其位置数据的哈希值的指针。一个普通的指针可以告诉你数据存储的位置，哈希指针不但可以告诉你数据存储的位置，并且还可以给你一种方式，让你验证数据没有被篡改过（见图1.4）。

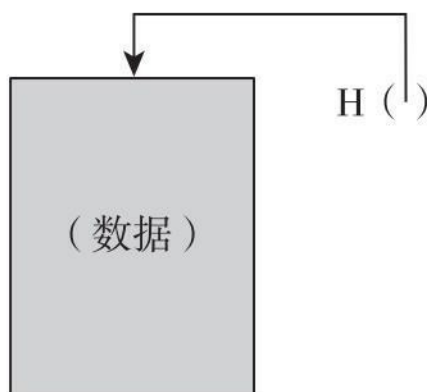


图1.4 哈希指针

注：哈希指针是一个不但可以指向数据存储的位置，还可以明晰某个时间戳下该数据的哈希值的指针。

我们可以利用哈希指针构建各种各样的数据结构。为求直观，我们可以把原来用普通指针实现的数据链表和二叉查找树通过哈希指针来实现。

区块链

如图1.5所示，我们通过哈希指针构建一个链表，我们将这个数据

结构称为**区块链**（block chain）。在普通链表中有一系列区块，每个a区块既有数据也有一个指向上一个区块的指针。而在区块链中，上一个区块指针被置换为哈希指针。因此，每个区块不仅能告诉我们上一个区块的值在哪里，还包含了该值的摘要，使我们能够验证那个值没有改变。我们存储链表头部（the head of list），即一个普通的哈希指针指向最近使用的数据区块。

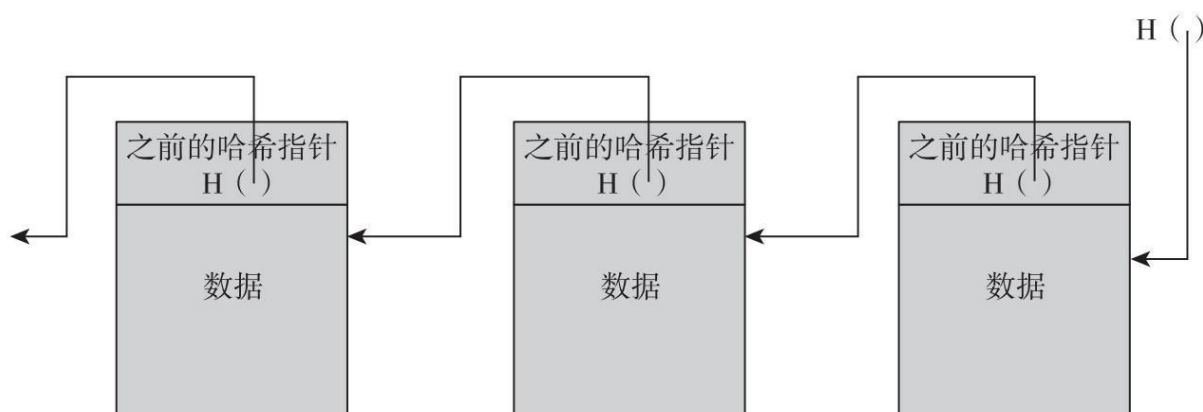


图1.5 区块链

注：通过哈希指针而不是普通指针构建的一个链表，我们把这个链表称为区块链。

区块链的一个应用就是“防篡改日志”。也就是说，我们要建立一个存储很多数据的日志数据结构，使我们能将数据附加到日志的末尾。但是如果有人篡改日志前面的数据，我们可以检测到。

要理解区块链如何实现这一防篡改特性，我们先看一下如果对手要篡改区块链中间的数据会发生什么。具体来说，通过这种方式，对手的目的是让只记得区块链头部哈希指针的人无法检测到篡改行为。为达到这个目标，对手会改变某区块k的数据。既然数据已经被改变，区块k+1的哈希值（即整个区块k的哈希值）将不会匹配。记住，因为哈希函数具有碰撞阻力，我们可以确定新的哈希值与改变后的内容不会匹配。因此，我们会检测到区块k中的新数据以及区块k+1中的哈希指针的不一致性。当然，对手可以继续尝试，并通过篡改下一个区块的哈希值掩盖这

次篡改。他可以一直这样做，但是当他到达链表的头部时，这个策略将会失败。具体来说，只要我们将链表头部的哈希指针存储在对手无法改动的地方，对手将不能做到在不被检测到的前提下，篡改任何区块（见图1.6）。

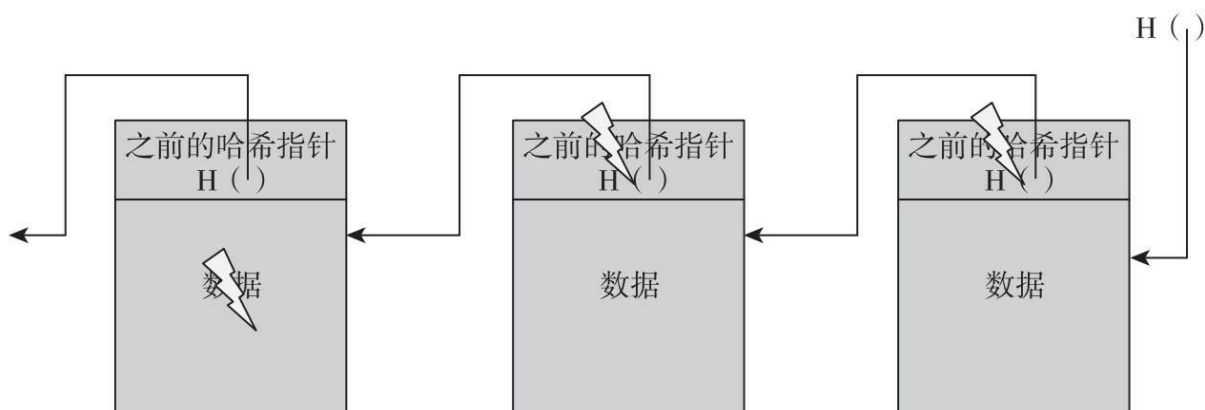


图1.6 防篡改日志

注：如果对手修改了区块链中的任意部位的数据，那么将会导致下一个数据块的哈希指针不正确。如果我们锁定区块链的头部数据，那么即使对手修改了所有哈希指针使其与修改过的数据一致，那么他也无法修改头部数据，从而我们就可以检测到篡改行为。

这样做的结果是，如果对手想要篡改区块链中任意地方的数据，为了保证整个内容一致，他需要篡改所有的哈希指针直至最开始的地方。他最终将碰到障碍，因为他不能篡改链表头部的指针。这样，我们便知道，仅通过记住一个哈希指针，我们就基本记住了整个链表的防篡改哈希值。因此，我们可以搭建一个包含很多区块的区块链网络，链表头部的哈希指针被称作**创世区块**（genesis block）。

你可能已经注意到了，区块链的结构与我们上一节见到的MD变换类似。的确，它们很相似，同一个安全论证对于两者都适用。

梅克尔树

另一个我们可以用哈希指针建立的有用的数据结构是二叉树。使用哈希指针的二叉树也叫作**梅克尔树**(Merkle trees)，以其发明者拉尔夫·梅克尔（Ralph Merkle）的名字命名。如图1.7所示，假设我们有很多包含数据的区块，这些区块就构成了树的叶子（节点）。我们将这些数据区块两两分组，然后为每一组建立一个有两个哈希指针的数据结构，每个指针对应一个区块，这些数据结构就构成了树的下一个层次。我们轮流将这些区块组两两分组，为每一组建立一个包含每个区块组哈希指针的新的数据结构。以此类推，直到我们得到一个单一区块，即树根节点。

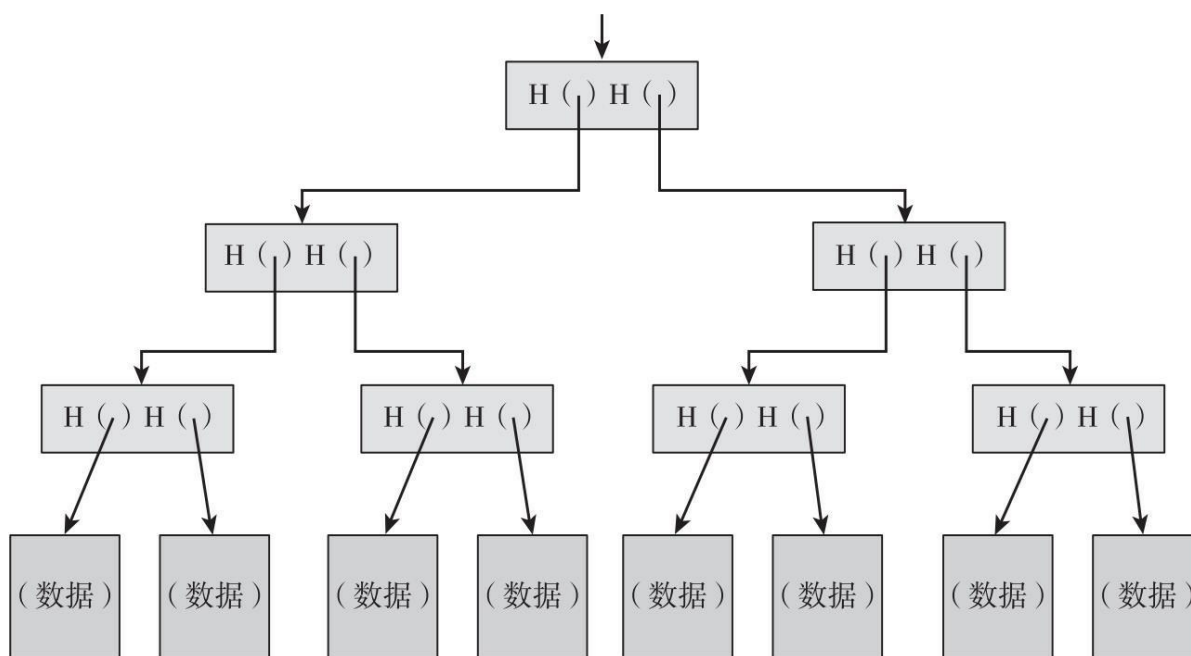


图1.7 梅克尔树

注：在梅克尔树的数据结构中，所有的数据区块都被两两分组，指向这些数据区块的指针被存储在上一层的父节点（parent node）中，而这些父节点再次被两两分组，并且指向父节点的指针被存储在上一层的父节点中，一直持续这个过程，直到最后我们到达树的根节点。

如上所述，我们要记住树最前面的哈希指针。我们现在可以通过哈希指针回溯到列表中的任何位置，这让我们能保证数据确实未经篡改，正如我们在区块链见过的一样，如果对手篡改了树底部的一些数据区块，会导致上一层的哈希指针不匹配，即使他继续篡改这个区块，改动

数据行为将最终传递到树的顶端，而此时，他将不能篡改我们存储的哈希指针。因此，同样地仅仅通过记住顶部的哈希指针，任何企图篡改任何数据的行为都会被检测到。

隶属证明

与我们之前建立的区块链不同，梅克尔树的另一个特点是它可以实现简洁的隶属证明。假设某人想要证明某个数据区块隶属于梅克尔树。同样地，我们只记住树根节点，然后他需要展示给我们数据块信息，以及从该数据区块通向树根节点的那些区块，我们可以忽略树的其余部分，这样做是因为这些区块已经足够让我们验证通往树根节点过程中所有的哈希值。其工作原理图解参见图1.8。

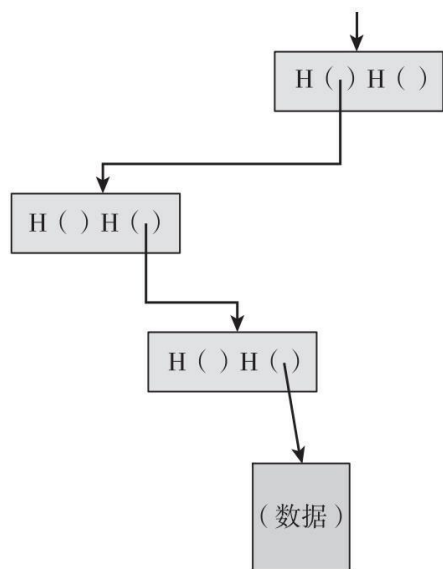


图1.8 隶属证明

注：为了证明某个数据区块来自一个梅克尔树，我们只需要找到该数据区块到树根节点的路径。

如果整棵树上有 n 个节点，只需要展示约 $\log(n)$ 个项目，因为每个步骤仅需要计算子区块的哈希值，验证过程需要时间约为 $\log(n)$ 。因此，

即使梅克尔树包含大量的区块，我们仍可以在相对较短时间内证明隶属关系。因此，验证需要花的时间和涉及空间（树节点）与 $\log(n)$ 同级。

一个排序梅克尔树是把底层的数据通过某些排序得到的梅克尔树，这里排序规则可以是字母表排序、词典排序、数字化排序，或者其他约定的排序方式。

非隶属证明

有了排序梅克尔树，我们可以在一个对数复杂度的条件下验证某一个数据区块并非来自某梅克尔树。也就是说，我们可以证明某个特定区块不属于梅克尔树，而我们只是简单通过展示被验证区块之前的区块路径，以及被验证区块之后的区块路径，就可以达到目的。如果之前、之后两个区块在树上连续的，那么这说明了被验证区块与该梅克尔树之间是非隶属关系。因为被验证区块确实隶属于梅克尔树，它需要在两个条目之间，而如果两个条目是连续的话，二者之间则并没有空间。

我们讨论过在链表及二叉树中使用哈希指针，但更广泛地说，我们可以在任何以指针为基础的数据结构中使用哈希指针，条件是数据结构不存在循环。如果数据结构中存在循环，那么我们将不能使所有哈希值得到匹配。想一下，在一个非循环的数据结构中，我们可以在靠近节点的地方开始，或者在没有指针的数据区块开始，计算其哈希值，然后从后往前进行计算。但是在一个有循环结构的网络中，并没有一个根节点，可以让我们去追溯。

因此，试想另一个例子，我们可以建立一个哈希指针定向的非循环图。

我们能够在该图中非常有效地验证隶属关系，同时也方便计算。这样的哈希指针使用方式是一个常见技巧，在分布数据结构中、在本章后

面会讨论到的算法中以及本书中都会反复提到。

1.3 数字签名

在本节，我们将讨论**数字签名**（digital signatures）。数字签名是密码学中的第二个重要部分，该理论和哈希函数一起，为我们后面讨论加密货币奠定基础。数字签名被认为是对纸上手写签名的数字模拟。我们对数字签名有两个特性要求，使其与我们对手写签名的预期一致。第一，只有你可以制作你自己的签名，但任何看到它的人都可以验证其有效性；第二，我们希望签名只与某一特定文件发生联系，因此该签名不能用于表明你同意或支持另一份不同的文件。对于手写签名来说，第二条就如同确保别人不能将你的签名从一份文件上剪下来，贴到另一份文件的末尾那样。

那我们如何通过密码学来构建这些性质呢？首先，让我们把之前的直观讨论说得更具体一些，以便今后可以更好地论证数字签名方案，并讨论其安全特性。

数字签名方案

数字签名方案由以下三个算法构成：

● $(sk, pk) := \text{generateKeys}(\text{keysize})$ `generateKeys`方法把`keysize`作为输入，来产生一对公钥和私钥。私钥`sk`被安全保存，并用来签名一段消息；公钥`pk`是人人都可以找到的，拿到它，就可以用来验证你的签名。

● $\text{sig} := \text{sign}(sk, \text{message})$ 签名过程是把一段消息和私钥作为一个输入，对于消息输出是签名。

● $\text{isValid} := \text{verify}(pk, \text{message}, \text{sig})$ 验证过程是通过把一段消息和签名消息与公钥作为输入，如果返回的结果是真，证明签

名属实；如果返回的结果为假，证明签名消息为假。

我们要求以下两个性质有效：

- 有效签名可以通过验证，即：

```
verify(pk, message, sign(sk, message))==true
```

- 签名不可伪造。

我们注意到generateKeys和sign都可以采用随机算法。的确，generateKeys最好是随机的，因为它需要为不同的人生成不同的密钥，而verify则需要是确定的。

现在，让我们更详细地检验我们要求数字签名方案具备的两个特性。第一个特性很直接，那就是有效的签名必须通过验证。如果我用我的密钥sk签署了一条消息，之后有人试图通过使用我的公钥pk验证关于同一条消息的签名，该签名必须证实为正确。这个特性是对签名有效的最基本要求。

不可伪造性。 第二个要求计算上不可能伪造签名。也就是说，知道你公钥并看到你在某些信息上签名的对手，不能伪造他还未见过的你在其他信息上的签名。这一不可伪造特性类似于我们与对手之间在进行一场游戏，游戏的使用在密码安全证明中很常见。

在不可伪造性游戏中，对手会声称他可以伪造签名，而挑战者会测试他所说的话（见图1.9）。我们做的第一件事是使用generateKeys方法生成一个密钥，以及相应的公共验证公钥，我们将密钥交给挑战者，然后将公钥交给挑战者以及对手。因此，对手只知道公共信息，而他的任务是试图伪造一条信息。挑战者知道密钥，因此他可以签名。

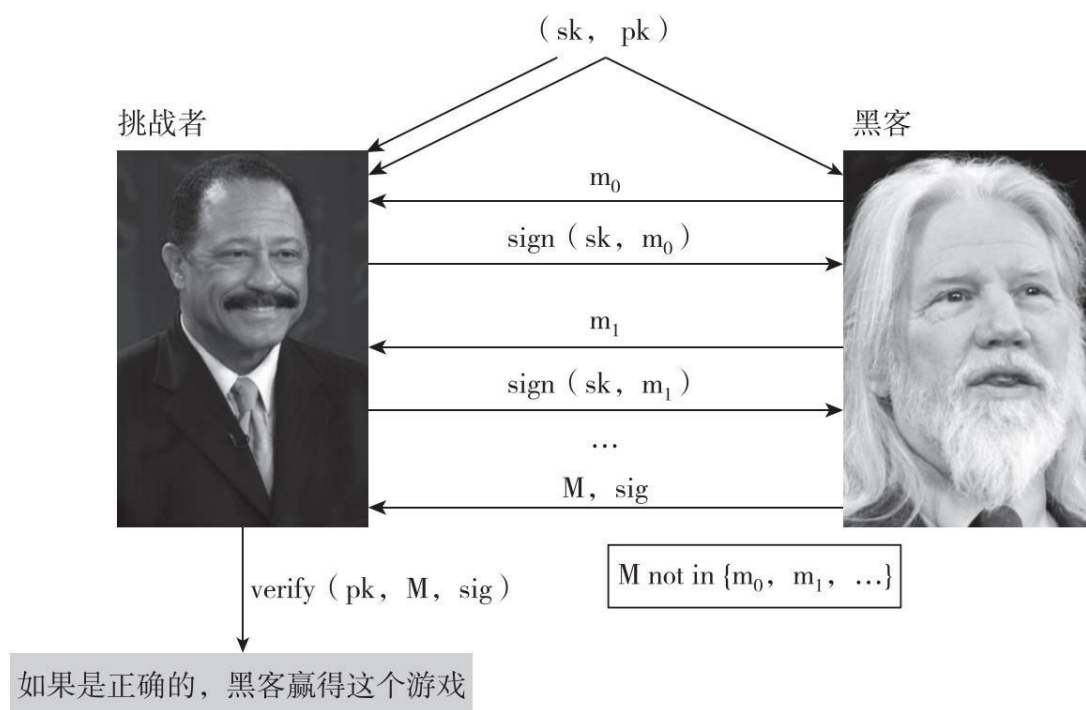


图1.9 不可伪造性游戏

注：不可伪造性游戏是对手（黑客）和挑战者一起玩这样一个游戏：如果黑客可以在一个之前没有见过的消息上进行签名，那么黑客就赢得这个游戏；反之，如果黑客做不到，挑战者就赢得游戏，从而可以证明这个数字签名方案是不可伪造的。

直观来看，这个游戏的设定与真实世界条件一致，现实中的攻击者很可能可以从潜在受害者的很多不同文件中看到有效签名，攻击者甚至还可能操控受害者签署一份看起来无害但对黑客有利的文件。

为了将这一点建模到我们的游戏中，我们将允许黑客选择一些文件的签名，不限时长，只要猜测的数量合情。合情猜测数量的意思是，我们允许攻击者尝试猜测的次数高达百万，但数量高达 2^{80} 就不行了。从渐进性角度来说，我们允许攻击者多次尝试，尝试次数可以是一个密钥大小的多项式函数，但次数不能更多（例如攻击者不能以指数方式猜测）。

一旦攻击者满意他所看到的签名数量，那他就可以挑选某条信息 M ，尝试在上面伪造签名。对 M 的唯一限制就是，它必须为攻击者之前

未在之上看过的签名的信息（因为很明显，攻击者可以发出他收到过的签名）。挑战者运行验证算法，以此确定攻击者生成的关于M信息签名在经过公共验证密钥验证后，是否属实。如果验证成功，攻击者赢得游戏。

不论对手使用什么算法，我们说签名方案不可伪造，当且仅当他成功伪造信息的机会非常小——小到我们可以假设在实践中从不会发生。

实践中的考量

要将算法概念转化为现实中可执行的数字签名机制，我们还需要考虑许多实际问题。例如，很多签名算法是随机的（特别是比特币使用的算法），因此我们需要随机性的良好来源。我们不能低估这一点的重要性，因为不良随机性会使你认为安全的算法变得不安全。

另一个实际问题是关于信息大小。在实践中，你能够签署的信息大小是有限制的，因为真实的方案将在位数长度有所限制的字符串中运行。有一个简单的方法可以解决这个限制：对信息的哈希值进行签署，而非对信息本身进行签署。如果我们使用输出值为256位的加密的哈希函数，那么我们可以有效地签署任何长度的信息，只要我们的签名方案能够签署256位的信息。如上所述，我们可以将信息的哈希值作为信息摘要，哈希函数具有碰撞阻力，因此这种方式是安全的。

我们后面会用到的另一个技巧是，可以对于哈希指针进行签署。如果你签署了哈希指针，那么该签名覆盖（或者说保护）整个结构——这不仅仅是哈希指针本身，还包括哈希指针指向的整个区块链。比如，如果签署了区块链末尾的哈希指针，其结果就是你有效地数字签署了整条区块链。

椭圆曲线数字签名算法

现在让我们来看一下具体的细节。比特币使用的数字签名方案叫作椭圆曲线数字签名算法（ECDSA）。ECDSA为美国政府的标准，是早前DSA^[1]算法利用了椭圆曲线的升级版。这些算法经过了数年的细致密码分析，且被普遍认为是安全的。

更具体地说，比特币使用ECDSA算法，而不是标准椭圆曲线“secp256k1”[预计提供128位安全保障，即打破这个算法的难度与执行 2^{128} 对称性密钥运算（如破解哈希函数）一样困难]。虽然这个曲线是公开标准，但除比特币以外鲜有使用，其他使用ECDSA的应用（如安全网络浏览时的TLS^[2]密钥交换）通常都使用更常见的“secp256k1”曲线。这就是比特币的一个古怪之处，因为在比特币系统早期实施中被中本聪选定（参见原版前言），现在已很难改变。

我们不会详细地讨论ECDSA的原理，因为这涉及一些过于复杂的数学知识，且对于本书的其他内容没有太多帮助。如果你对ECDSA感兴趣，请参见本章末尾延伸阅读部分。虽然我们这么说，但对于了解各种参数也许会很有必要：

个人密钥：256位

公钥（未压缩）：512位

公钥（压缩）：257位

待签名信息：256位

签名：512位

注意，严格来讲，虽然ECDSA只能签署256位的信息，但这存在问题，因为信息在签署之前总是已经经过哈希压缩，因此，任何大小的信

息都能被有效签署。

使用ECDSA时，确保随机性良好来源至关重要，因为不良来源将可能导致密钥信息的泄露。这一点不难理解，如果你使用了不良随机来生成密钥，那么该密钥就可能不安全。但是ECDSA的古怪就在于，即使你仅仅只是在生成签名时使用了不良随机，而你使用的密钥完美无缺，你的个人密钥还是有可能泄露（熟悉DSA的人都知道这是DSA的古怪之处，但并不针对椭圆曲线）。接着游戏就结束了，如果你的个人密钥泄露，对手就可以伪造你的签名。因此，我们在实践中要特别注意使用良好随机来源，使用不良随机来源是安全系统的一个常见缺陷。

数字签名作为密码学基础，我们对其讨论就此结束。在下一节，我们将讨论对打造加密货币会带来帮助的一些数字签名应用。



加密货币及加密术

如果你一直在期待比特币使用的加密算法，我们可能会让你失望了，比特币并没有使用任何加密术，因为并没有加密的需要。加密术只是因为现代密码学而变得可能成为众多技术中的一个，很多技术（如承诺方案）在某种程度上隐藏信息，但是与加密术有所不同。

[1] DSA (Digital Signature Algorithm)，电子签名算法。——译者注

[2] TLS (Transport Layer Security)，传输层安全协议，用于在两个通信应用程序之间提供保密性和数据完整性。——译者注

1.4 公钥即身份

让我们来看一下与数字签名并行的一个有用技巧，基本想法是从数字签名模式中拿出一个公共验证密钥，并将其与一个人或一个系统参与者的身份对等。如果你见到一条消息的签名被公钥pk正确验证，那么你可以认为pk就是在表达这条消息。你真的可以将公钥认为是参与者或者系统的一方，他可以通过签署声明而发布声明。从这个角度来说，公钥就是身份，让某人能为pk身份发声，他必须知道相应的密钥sk。

将公钥视为身份的一个结果是，你可以随时制定新的身份——你可以简单通过数字签名方案中的generateKeys程序，生成新的密钥对sk和pk。pk是你可以使用的新的公共身份，sk是相应的密钥，只有你自己知道并可以让你代表身份为pk发声。在实践中，你可能会使用pk的哈希作为你的身份，这是因为公钥很大。如果是这样的话，为了验证消息来自你的身份，人们会需要验证：（1）你的身份确实是pk的哈希；（2）信息能经过公钥pk验证。

此外，在默认情况下，你的公钥pk基本上看起来是随机的，也并没有人能够通过检查pk发现你的现实身份（当然，一旦你开始使用这个身份发表声明，这些声明可能泄露信息，而让别人将你的真实身份与pk联系起来。我们很快会更详细地讨论这个问题）。你可以生成一个看起来随机的新身份，看起来像人群中的一张脸，但这些都只有你能够控制。

去中心化身份管理

公钥和私钥的体系，帮助我们引入去中心化的身份管理的理念。你可以自己作为用户注册，而无须到一个中央机构注册为系统用户。你不

需要别人给你一个用户名，你也不需要告诉任何人你会使用什么名字。如果你想要新的身份，可以随时生成一个，而且想要多少就生成多少。如果你希望拥有五个不同的名字，没有问题！那就生成五个身份。如果你想匿名一阵子，你可以生成一个新的身份，使用一段时间，然后弃之不用。有了去中心化身份管理，所有这一切都变得可能。事实上，这就是比特币对待身份的方式。这些身份在比特币语言中被称为地址。你可以常常听到地址这个词，用于比特币或加密货币相关的内容中，而地址其实就是公钥的哈希值。作为去中心化身份管理方案的一部分，它就是某人凭空捏造的一个身份而已。



安全性与随机性

你可以不经过中央机构而生成一个身份的概念可能看起来有悖常理。毕竟，如果有人刚好就生成了跟你一样的密钥，他不就能偷走你的比特币吗？

我们给你的回答是，别人生成一个与你的相同256位密钥的概率如此之小，在实践中，我们不需要担心它会发生。总而言之，我们保证这种情况绝不会发生。

一般来说，与新手的直觉不同的是，概率系统是不可预测且难以推理的，反面的常常是真的——统计学理论使得我们可以精确地量化我们感兴趣的事件的概率，并对该系统行为做出自信的推论。

但还有一个精妙之处：概率保证只有在密钥为随机产生时为真。在现实系统中，随机的生成常常是薄弱环节。如果两个用户的电脑使用同样的随机来源或者使用可预测的随机，那么理论保证不再适用。所以，在生成密钥时使用良好随机源至关重要，以确保实践保证与理论保证相符。

乍一看，去中心化身份管理可能极具匿名性及隐秘性。毕竟，你可以自己创建一个看起来很随机的身份，同时也不用告诉任何人你的真实身份是什么。但事实并不是这么简单，随着时间的推移，你创建的身份会做出一系列的声明。人们看到这些声明便知道拥有这个身份的人做出了特定的一系列行为。他们能够开始将细节联系起来，从这一系列的行为推断出你的真实身份。随着时间的推移，一个观察者可以将这些事情联系起来，并推断出这样的结论：“天，这个人的行为好像乔（Joe），可能这个人就是乔。”

换句话说，在比特币系统中，你不需要明确地注册或揭露你的真实身份，但是你的行为模式本身可能是可识别的。这就是比特币等加密货币的基本隐秘性问题，我们将会在第6章专门讨论这个问题。

1.5 两种简单的加密货币

现在，让我们从密码术过渡到加密货币。我们之前的密码术干货在这里就要开始发挥作用了，今后我们会逐渐看到各部分之间如何相互联系，也会发现哈希函数和数字签名等密码程序的意义。在本节，我们将讨论两种很简单的加密货币。当然，我们也需要学习本书后面大量的内容，才能深刻阐释比特币本身的运作机制。

高飞币

第一个是高飞币（GoofyCoin，此币的创造者叫高飞），它应该是我们能想到的最简单的加密货币。高飞币只有两个规则，第一个规则是指定高飞可以随时创建新币，且这些新创建的币都属于他。

为创建新币，高飞生成一个他之前从未生成的唯一的货币编号（uniqueCoinID），并建立字符串“CreateCoin [uniqueCoinID]”。然后，他使用秘密签署密钥计算这个字符串的数字签名，该字符串与高飞的签名就构成一单位币。任何人都可以验证该新币包含高飞有效签名，因此该新币为有效币。

高飞币的第二个规则是，拥有此币的人可以将其转给其他人。转移一只币不是简单地将币数据结构发送给接受者，而是必须通过密码程序来完成。

假设高飞想把他创建的一只币转给爱丽丝。未达成这个目的，他需要创建一个新的声明表示“将此币支付给爱丽丝”，在此声明中“此币”就是该币的哈希指针。如上所述，身份其实就是公钥，因此“爱丽丝”指的

就是爱丽丝的公钥。最后，高飞签署代表该声明的字符串。因为高飞是起初拥有该币的人，他必须签署花掉该币的任何交易。一旦由高飞签署的代表他的交易的这个数据结构存在，爱丽丝便拥有这个币。她可以向任何人证明她拥有这个币，因为她可以展示有高飞有效签名的数据结构。此外，它也指向曾经为高飞所有的一个有效币。因此，该币的有效性及所有权在系统中就不言自明了。

一旦爱丽丝拥有了这个币，她也可以花掉它。为达到这个目的，她创建了一个声明表示“将这个币付给鲍勃的公钥”，此时“这个币”就是她所有的那个币的哈希指针。当然，爱丽丝要签署该声明。任何看到这个币的人都可以验证鲍勃是其所有人。他们可以根据哈希指针链追溯到该币的创建及验证每一个步骤，这就是其合法所有人签署了一份声明表示“将这个币支付给 [新的所有人]”，详见图1.10。

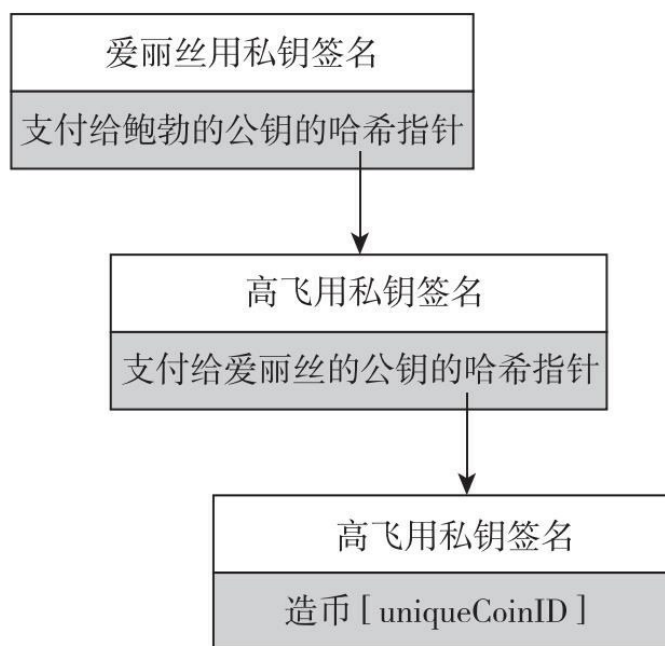


图1.10 高飞币交易

注：该图示例了货币创造的过程和被花费过两次的过程。

总结一下，高飞币的规则是：

● 高飞可以通过签署声明表示他使用唯一的货币编号来创建一个新币。

● 币的所有人可以通过签署声明表示“将这个币转给X”（其中X为公钥），将其转给另一个人。

● 任何人都可以验证一只币的有效性，跟随哈希指针追溯到它是由高飞创建，并验证过程中所有签名。

当然，高飞币有一个致命安全隐患。假设爱丽丝通过把她签署的声明发送给鲍勃，即将她的币转给鲍勃，但并没有告诉其他人。她也可以创建另一个签名，声明将同样一只币转给了查克（Chuck）。对于查克来说，这看起来是一个完全有效的交易，而他是该币的所有人。鲍勃和查克似乎都可以有效表示自己是那个币的所有人。这个就是所谓的**双重支付**（double spending）——爱丽丝将同样一只币花了两次。我们一看就知道货币是不能这样花的。

事实上，双重支付是任何加密货币需要解决的主要问题之一，高飞币没有解决这一问题，因此不安全。

高飞币很简单，其货币转移机制其实与比特币非常相似，但是因为它并不安全，因此并不适合作为加密货币。

财奴币

为解决双重支付问题，我们会涉及另外一个加密货币，我们将其称为财奴币（ScroogeCoin）。财奴币是以高飞币为基础创建的，但在数据结构方面更复杂。

第一个主要概念如下：一个叫财奴的指定实体将负责公布包含所有

发生过的交易历史记录的唯一账目（append-only ledger），账目的仅增特性保证了写入这个账目的任何数据都会永久保留下来。如果账目真的为仅增，通过要求所有的交易在被接收前都写入项目，我们可以用其防止双重支付的发生。这样，如果之前币已经转给了一个不同的所有者，大家都可以看到。

为执行这个仅增功能，财奴可以建立一个区块链（我们之前已经讨论过其数据结构），对于区块链，财奴要进行数字签名，因此，这从而就形成了一系列数据块，每个数据块都包含一次交易（在实践中，一种优化的做法是将多次交易放入同一个区块中，比特币就是这样做的），每个区块包含交易的ID、交易的内容，以及上一个区块的哈希指针。财奴数字签名是针对最后一个哈希指针（它约束整个结构中所有的数据），并将签名与区块链一起发布，见图1.11。

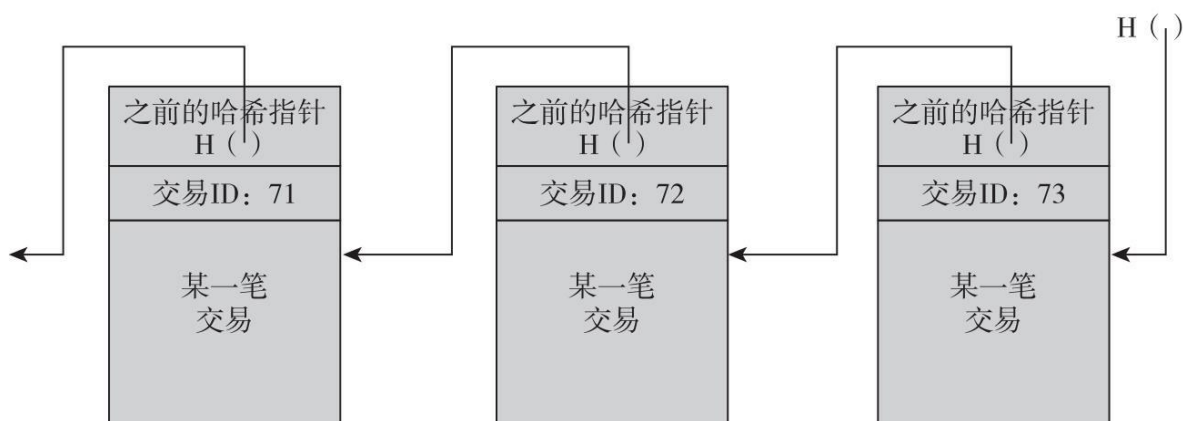


图1.11 财奴币系统中的区块链

在财奴币中，只有在由财奴签名的区块链的交易才算数。任何人都可以通过核查财奴在区块中的签名来验证交易是否经过财奴的支持，财奴会确保不会支持企图双重支付，也就是不会支持已经支付过的币的交易。

为什么除了让财奴签署每个区块，我们还需要一个带哈希指针的区块链？这样做是保证仅增特性。因为财奴有可能试图增加或移除交易记

录，或者改变已有交易，而一旦有了哈希指针，将会影响到后面所有的区块。只要有人监督财奴发布的最新哈希指针，变化会很明显，并可以被轻易发现。在一个财奴分别签署不同区块的系统中，你需要记录他签署的每一个签名。采用区块链，两个不同的人可以轻易验证他们确实观察到了同样的，由财奴签署的交易记录。

财奴币中有两种交易。第一种是造币（CreateCoins），类似于在高飞币中，高飞可以创建新币的程序，而财奴将其进行了扩展，那就是可以在一次交易中创建多个币量，见图1.12。

交易ID: 73		类型: 造币	
被创造的货币			
序号	数量	造币记录	
0	3.2	0x...	←—— 虚拟货币ID 73 (0)
1	1.4	0x...	←—— 虚拟货币ID 73 (1)
2	7.1	0x...	←—— 虚拟货币ID 73 (2)

图1.12 造币交易

注：造币交易创造多个货币。每一个货币在交易中都有一个序号。其次，每一个货币也有一定的数量，来对应某个数目的财奴币。最后，每一个货币还有一个造币记录，在货币被制造出来的时候对应的公钥。因此，造币交易创造了多个不同数量和归属于不同拥有者的新货币。我们将这些货币称为虚拟货币ID，指的是该次交易中交易ID和货币序号的组合。

造币交易如果是由财奴签署，从定义上说它总是有效的。我们不会担心财奴什么时候有权创建新币或者可以创建多少，正如我们不担心在高飞币中，高飞可以创建新币那样。

第二种交易是付币（PayCoins）。这一交易会消耗币，就是说消除它们，并创建具有相同总值的新币。新币可能属于不同的人（公钥），这一交易必须由每一个支付该币的人来进行签署。因此，如果你是本次

交易中将会消耗的某只币的所有人，那么你就需要数字签署该交易，表明你同意花掉这只币。

财奴币的规则阐明，如果以下四个条件为真，付币交易有效：

- 被消耗的币为有效货币，即它们是在之前的交易中创建的。
- 被消耗的币没有在之前的某交易中被消耗掉。就是说，本次交易不是双重支出。
- 本次交易产生的币值量等于消耗的币值量，也就是说，只有财奴才可以创建新币。
- 本次交易被消耗的所有币均有其所有者的有效签署。

交易 ID: 73		类型: 付币
消耗的虚拟货币 ID: 68 (1), 42 (0), 72 (3)		
被创造的货币		
序号	数量	造币记录
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
签名		

图1.13 付币交易

如果所有条件都满足，那么付币交易有效，并且财奴会接受交易（见图1.13）。他会通过将其附加到区块链上，将交易写入历史记录。之后，每个人都可以看见交易发生了。只有在这时，参与者才可以接受交易实际发生了。直至发布之前，它都可能是一个被双重支付抢占的交

易，即使前三个条件都被满足。

这个系统中的货币是不可变的——它们不会被改变、细分或者联合。每个币都在一次交易中被创建一次，然后在之后的其他交易中被消耗。但是我们可以通过交易对货币进行细分或联合，来实现相同的效果。例如，为了细分一只币，爱丽丝创建了消耗该币的新交易，然后生成了两个具有同样总值的新币，这两个新币可以再次分配给她。因此，虽然在本系统中币是不可变的，但是它具有除了可变币以外的系统的所有灵活性。

现在，我们来看一下财奴币的核心问题，财奴币的工作原理是人们可以看见哪些币是有效的。它防止双重支付，因为每个人都可以查看区块链，看到所有交易都是有效的，每一只币确实都只被消耗了一次，但其问题是，财奴的权利太大了。他虽然不能创建虚假交易，因为他无法伪造其他人的签名，但是他可以停止支持其他用户的交易，不为他们提供服务并让他们的货币无处可花。如果财奴是贪婪的（正如与他同名的卡通形象一样），他可以拒绝公开交易，除非其他人向他支付强制性交易费。当然了，财奴还可以想要多少币，就给他自己创建多少。或者财奴也可能厌倦整个系统，因此完全停止更新区块链。

这里的问题就是中心化。虽然财奴本身满意这个系统，我们用户可能会不满意。财奴币虽然看似是一个不切实际的方案，但是在很多早期的密码系统研究中，确实假设过一些中央可信机构，还特别被称为银行。毕竟，绝大多数现实世界货币的确有可信发行人（通常为政府造币厂）负责创建货币，并决定哪些钱币为有效货币。但是，具有中央机构的加密货币纷纷在实践中失败。原因有很多，回头来看，我们似乎很难让人们接受有中央机构的加密货币这个事物。

因此，为改善财奴币，并建立一个可行系统，我们需要解决的主要技术问题是：我们是否能让系统“去财奴化”？也就是说，我们是否能放弃中心化的财奴人物？我们能够有一个在很多方面像财奴币一样运作的

加密货币，但没有中央信任机构吗？

为回答这些问题，我们需要解决所有用户如何在交易历史记录发生后，一致同意采用一个公开区块链，他们必须一致同意哪些交易有效、哪些交易是实际发生了。他们还需要能够用一种去中心化的方式分配ID。最后，新币的铸造也需要通过去中心化的方式进行掌控。如果我们解决所有这些问题，那么我们可以创建一个如同财奴币那样的货币，但确实没有中心化的机构。实际上，这样的一个系统就与比特币非常相像了。

延伸阅读

史蒂芬·列维（Steven Levy）的《密码术》，从一个令人愉悦的、非技术的角度看待现代密码术的发展，及其背后的人和事：

Levy, Steven. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. London:Penguin, 2001.

现在密码术还是一个较为理论化的领域，密码学者使用数学以一种较为正规的方式定义其基础知识、协议以及其他被用户期望的安全特性，并根据关于特定数学问题的计算复杂性中被广泛接受的假设，来证明它们的安全性。本章我们使用到了直觉语言来讨论哈希函数及数字签名。对于有兴趣用更为严格的数学的方式，以及想更深入探索这些概念及其他密码学理论的读者，我们推荐你阅读：

Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography*, second edition. Boca Raton,FL:CRC Press, 2014.

对于应用密码学概述，参见：

Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. *Cryptography*

Engineering: Design Principles and Practical Applications. Hoboken,NJ:John Wiley & Sons, 2012.

精读定义SHA-256的NIST标准是了解密码学标准的有效方式:

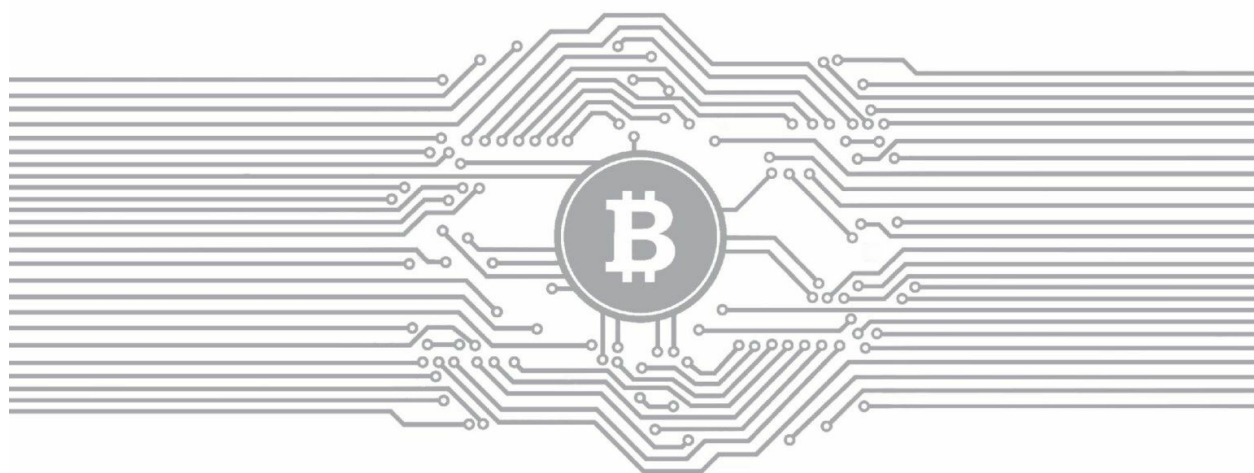
NIST.“Secure Hash Standards, Federal Information Processing Standards Publication.”FIPS PUB 180-4. Information Technology Laboratory, NIST, Gaithersburg, MD, 2008.

最后, 请参考讨论ECDSA签名算法标准化版本的论文:

Johnson, Don, Alfred Menezes, and Scott Vanstone. “The Elliptic Curve Digital Signature Algorithm (ECDSA).” International Journal of Information Security 1 (1) 2001:36-63.

第2章

比特币如何做到去中心化



在这一章，我们将讨论比特币如何做到去中心化。在第1章中，我们讨论了比特币底层加密算法的基础，最后我们谈到了财奴币。作为一种以账本为基础的记账式加密数字货币，财奴系统已经做得确实不错了，但它有一个很突出的问题，那就是该系统非常依赖一个被称为“财奴”的中心化权威。在第1章的最后，我们提出了财奴币去中心化的问题，或者说如何去财奴化。在本章，我们将着重讨论这个问题。

通读完本章，我们将注意到比特币并不是完全使用纯技术手段，而是将技术手段与一种明智的激励机制相结合，做到了去中心化。本章的最终目的会使你对去中心化有一个通盘的认识，同时也对比特币运作机制有所了解，并且懂得为什么比特币确实是安全的。

2.1 中心化与去中心化

去中心化是一个重要概念，这个概念并不是比特币独有的特性。在各种数字技术领域，中心化与去中心化两派的竞争也越来越多见。为了更好地理解竞争模式在比特币里的表现，我们有必要了解一下两派竞争在其他不同技术领域的竞争焦点。

互联网其实就是一个著名的去中心化系统。但在早期，互联网是在与美国在线（American On-Line，简称AOL）以及CompuServe^[1]等围墙花园式信息服务体系的竞争中，逐步变得越来越风行。电子邮件的实质也是一种简单邮件传输协议（Simple Mail Transfer Protocol，简称SMTP）的去中心化系统。尽管电子邮件也受到像脸书（Facebook）、领英（LinkedIn）这些中心化私有信息系统邮箱服务体系的挑战，但电子邮件仍然是人与人之间进行通信的一种被默认的选择。其实，我们已经不能简单将像即时短信或者短信等通信手段归类为是中心化，或者是去中心化模式，这些通信方式往往是一种混合模式。在社交网络中，尽管有很多爱好者、技术开发人员，甚至还有企业者也在尝试用去中心化的方式来替代像脸书、领英这样的中心化系统，但目前这些中心化系统仍具统治地位。事实上，中心化与去中心化的竞争在数字时代之前就已经存在，在电话、无线电、电视及电影的发展史上，我们都曾看到过这两种模式的竞争。

中心化与去中心化也并非水火不容，其实没有一个系统是完全中心化，或者是完全去中心化的。比如，电子邮件其实是一个去中心化系统，它基于一个标准的中心化协议SMTP，任何人只要愿意，都可以设计一个自己的电子邮件服务器。但实际情况是，只有一小部分电子邮件服务商在这个领域占据着统治地位。类似，虽然比特币系统是去中心化的，但比特币交易所（将比特币转换成其他货币的平台）、钱包软件以

及用户管理比特币的软件，可以是中心化的，也可以是去中心化的。

有了以上的考虑，我们把比特币如何做到去中心化这个问题拆解为下面五个问题：

- 1.谁在维护交易账本？
- 2.谁有权利批准哪个交易是正当有效的？
- 3.谁在制造新的比特币？
- 4.谁在制定系统变化规则？
- 5.比特币是如何取得交易价值的？

前三个问题反映了比特币协议的技术细节，我们将在本章重点讨论。

比特币系统的不同方面是从不同点涉及了中心化及去中心化。点对点网络是最接近去中心化的体系，任何一个人都可以运行一个比特币节点，而且基本没有什么入门门槛，用户只需要上网下载一个比特币客户端，就可以在其个人电脑上运行一个节点，现在全球有成千上万个这样的节点。在本章2.4节中我们将要学习比特币挖矿（bitcoin mining），从技术上讲，挖矿过程也是向所有人开放的，但挖矿需要很多资金投入。正因为如此，挖矿领域具有非常高的中心化及挖矿能力集中的倾向。比特币社区里有许多人认为这种现象并不可取。第三点是关于比特币运行节点软件的更新，这涉及何时以及如何更新系统规则。大家可以想象，就像电子邮件系统那样，这些节点可能有各种根据相同方式但通过不同手段实现的不同版本。但在实际上，绝大多数节点用的都是社区里被大家公认的有权威的资深开发者开发出来的软件。

[1] CompuServe，美国最大的在线信息服务机构之一。CompuServe产品于1979年问世，它

提供留言板、新闻和信息、电子商务以及其他类似网络功能的服务。这款产品的问世时间远远早于网络。美国在线在20世纪90年代早期的崛起，使得CompuServe退居美国第二大在线服务商。不久之后，CompuServe不得不同互联网进行竞争，它变成了一个不那么令人满意的互联网服务提供商。而且，随着用户更多地使用互联网，CompuServe风光一时的留言板也开始被人抛弃。1997年，美国在线收购了CompuServe。正如网景一样，CompuServe成为美国在线用在其他产品上的标示。现在，CompuServe只是一个半门户网站。——译者注

2.2 分布式共识

在前一节，我们笼统地讨论了去中心化和中心化。现在我们从一个更为技术性的层面看一下比特币的去中心化。接下来，我们会遇到一个被称作“共识”（consensus）的重要概念，特别地，还有“分布式共识”（distributed consensus）。建立一个分布式的电子现金系统的关键技术问题，就在于要达成分布式共识。直观地说，你可以想象我们的目标就是要将第1章提到的财奴币去中心化。

分布式共识有各种应用，计算机界对其也研究了多年，传统具有启发式的应用就是提高分布式系统的可靠性。设想你在管理一个社交网络公司的后端平台，比如微信，像这样庞大的系统通常有几千台甚至几万台服务器，这些服务器组成了一个巨大的分布式数据库，数据库中记录了这个系统里发生的各种活动，而每条信息都会被记录在后端的若干个节点上，对于整个系统的状态，这些节点必须要做到同步。

分布式共识协议的意义远远超出了传统意义的范畴。一旦具备了这样的体系，我们就可以建立一个庞大的分布式**键值**（key-value）存储库，该类存储库可以将任意数据如身高、名字等对应一个相应的开启键，基于此，许多应用得以实现。例如，我们可以建立一个分布式域名系统，将人脑易于理解的域名与IP地址进行配对，我们也可以建立一个公钥目录，这个目录可以把公钥与电邮地址（或者其他真实世界中的身份证明）对应起来。

以上讨论在直觉上说明了分布式共识的大概含义。对于分布式共识，我们还是要给出一个技术定义，以此我们可以判别一个协定是否符合分布式共识的要求。

分布式共识协议 在一个有n个节点的系统中，每一个节点都有一个输入值，其中一些节点具有故障，甚至是恶意的。一个分布式共识协议有以下两个属性：

- 输入值的中止须经所有诚实节点来确定。
- 这个输入值必须由诚实节点来生成。

那么以上概念在比特币里又是什么含义呢？想要理解分布式共识在比特币中的用途，我们需要记住比特币是个点对点的系统。当爱丽丝向鲍勃付款的时候，她其实是在向构成比特币网络上的所有节点广播其交易行为，见图2.1。

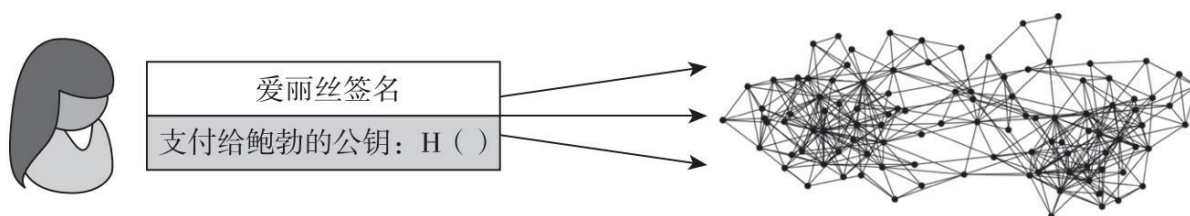


图2.1 广播交易

注：为了向鲍勃付款，爱丽丝需要向整个比特币点对点网络进行广播。

顺便提一下，你可能注意到，当爱丽丝向整个比特币点对点系统广播时，鲍勃的计算机并不一定在图2.1的网络中。当然鲍勃也有可能在这个网络上运行着一个节点，如果鲍勃想在爱丽丝转币给他时及时被系统通知，运行一个节点当然是个好主意，但其实这并不重要，鲍勃是否运行节点并不影响他收到爱丽丝转给他的比特币。

在比特币网络里，节点到底要达成什么样的共识呢？网络里有各种各样的用户在向网络广播交易，节点必须对哪些交易可以进行广播和交易发生的次序达成共识，以此系统将形成一个唯一的全球交易总账。回想我们在第1章1.5节中曾提到的财奴币将交易打包成块，对信息进行优

化处理。类似地，在比特币体系里，我们也将每个区块进行共识处理。

在任何时点，所有在点对点网络上的节点都有包含一系列区块的总账本，每个区块中都包含了已经被所有节点达成共识的交易清单。除此之外，每个节点还有一堆没有被打包进入区块的交易，就是那些网络节点已经被通知、交易已经发生，但还没有被写进区块的交易。网络节点对于这些交易还没有达成共识，所以每个节点都有一个略有差异、尚待确认的交易池。在实际中，点对点网络是不完美的，所以有些节点听到了交易，而有些节点却没有听到。

那么，所有的节点是如何对一个区块达成共识的呢？一个方法是，在一个时间段里，比如说每隔十分钟，每个节点都提议，自己的未被认可的交易成为已经达成共识的区块链后面的下一个区块，然后那些节点会执行一些共识协议，每个节点把自己提议的区块作为输入。但不可避免地，有些节点可能是恶意的，存心要把不当交易放进区块里，其他节点则是诚实的。如果共识协议能够顺利完成，一个正当有效的区块会被选作输出值。尽管有些被选出的区块是由一个节点提交，但只要这个区块是正当有效的，输出就是正当有效的。这时候可能有人会指出，这个被选出的区块可能未包含所有的正当有效的交易，但这并没有关系，如果有些正当有效的交易没被放进区块，它们可以等待下一次机会。

前面所谈到的这个办法与比特币系统有些相似之处了，但实质还是不完全一样。以上做法有几个技术上的问题：第一，达成共识一般是个难题，因为有些节点会死机或是根本就是恶意节点；第二，就比特币而言，点对点网络是不完美的，并非所有对应的节点是两两相连的，互联网链接的不良可能会造成网络问题，要执行一个所有节点都参与的共识协议好像并不现实；第三，由于交易信息是分布在整个互联网上，信息传递会有严重延迟。



延迟与全球时间

比特币协议达成共识时必须直面两大障碍：其一是不完美网络，例如信息延迟和节点死机，其二是某些故意搞破坏的节点。

严重网络延迟导致的一个后果是，节点之间没有一个统一的全球时间概念。意思是，并非所有节点都能根据每个交易的时间戳来达成交易时间共识，因此，共识协议不能执行以下指令：“在第一步里发了第一个消息的节点必须在第二步里执行X。”这一做法根本无法执行，因为所有的节点对于谁在第一步中发出第一个信息有不同的看法。

不可能性结论

在全球时间上的不统一，给共识协议算法带来了很大限制。事实上，由于这些限制，许多关于分布式共识的文献都对是否能达成共识持悲观态度，有许多达成共识具备不可能性的结论已经被证实。一个经典案例就是“拜占庭将军问题”（Byzantine Generals Problem），这个经典难题是这样阐述的：拜占庭是东罗马帝国的首都，它的军队分成多个师，每个师都由一个将军统领。这些将军通过信使进行交流，来达成一个共同作战方案，有些将军可能是叛徒，想故意破坏这个过程，这会造成那些忠诚的将军也无法达成一个统一的作战计划。解决这个难题的办法就是让那些忠诚的将军在这样的情况下达成统一作战方案，而避免那些叛徒对作战方案的误导。事实证明，如果叛徒数量超过1/3时，这个难题将无法克服，那些忠臣的计划终会被叛徒们破坏。

还有一个更为微妙的关于不可能性的结论，这就是著名的“Fischer-Lynch-Paterson不可能结果”[\[1\]](#)，该名称以最初的作者而命名。该结果指出，在一定的条件下（包括节点行为具有确定性特征），甚至在只有一个缺陷的过程中，达成共识都是不可能的。

尽管有这些“不可能性结论”，还是有文献谈到了一些共识协议。比较著名的就是Paxos算法协议。Paxos算法做了一些妥协，一方面，Paxos算法能做到不产生不一致的结果；另一方面，Paxos算法所做的妥协是，在一定条件下（虽然是不常见的情形），该协议会死机卡住，从而无法继续运行。

打破传统上的假设

但好消息是，这些所谓的“不可能性结论”都是在一些特定的模式下才成立，这些结论是针对分布式数据库的研究，这些模型不能完全套用到比特币身上来，比特币本身就打破了很多原来分布式数据库所做的假设。这些结论其实从某一方面让我们更明白了那些特定模式，由此或许可以真正对分布式共识给出解决方案。

具有讽刺意义的是，就目前对共识的研究来说，比特币实际运行情况下远比理论上告诉我们的要好得多，这就是比特币让专家们跌破眼镜之处。我们看到分布式共识在比特币里运行良好，但我们还没有建立理论来充分解释为什么会这样，但无论如何，完善理论对将来的发展还是十分重要的，理论结果可以使我们预测，甚至预防未来可能的攻击和问题。我们一旦具备了较强的理论依据，来解释比特币分布式共识的良好运作机制，我们才能真正地对比特币的安全性和稳定性做出保证。

比特币到底打破了经典模型里的哪些假设呢？第一，比特币引进了奖励的理念，这对分布式共识协议来说是一个全新的理念，这也只有在

比特币里才可能实现，因为比特币也是个货币，所以人们自然而然地会为了金钱奖励而变得诚实起来。所以，比特币并没有真正解决分布式共识问题，它只是在特定货币系统下解决了这个问题而已。

第二，比特币体系包含随机性这个概念。在后面两节里我们将会看到，比特币的共识算法很大程度上依赖于随机性。此外，它也不再纠结于规定共识的起点与终点。相反，共识是通过一段较长的时间而达成的，在实际系统中，达成共识大约需要一个小时左右。但即使在一个小时以后，节点们也无法确定哪一个交易块应该进入总账本。但随着时间的流逝，我们对某一个块的认识与最终总体共识相吻合的概率将越来越大，观点出现分歧的概率按指数级下降。比特币在以上方面的不同，让它能够逾越传统理论关于分布式共识不可达成这一鸿沟。

[1] Fischer-Lynch-Paterson不可能结果，是Michael J. Fischer、Nancy A. Lynch和Michael S. Paterson在论文Impossibility of distributed consensus with one faulty process中证明的一个结论，称得上是分布式理论中最为深刻的结论，大致表述如下：“在一个多进程异步系统中，只要有一个进程不可靠，那么就不存在一个协议，此协议能保证有限时间内使所有进程达成一致。”——译者注

2.3 使用区块链达成没有身份的共识

在这一节里，我们将探讨比特币共识算法的技术细节。回忆一下，我们在前面曾说过，比特币中的每个节点并没有一个稳定的、长期的身份，这一点也是与传统分布式共识算法的不同之处。身份缺失的原因是，在一个点对点网络中，没有一个中央权威机构来发放身份，并保证它们没有制造节点。用技术术语来说，乱造节点就是所谓的“女巫攻击”（sybil attack）现象。女巫就是恶意黑客制造的不同节点，这些节点看起来像是对应不同的身份的人，其实是由一个人在幕后控制。另一个原因是化名制（pseudonymity），也是比特币想达到的一个目标，所以即使可以替所有节点建立唯一真实身份，我们也不想那样做。虽然比特币还是不能保证真正的匿名，一个用户用不同身份做的不同交易还是有办法被最终追踪到，但比特币的特性毕竟没有强迫大家用真实身份来加入。这是比特币的重要特性，也是比特币系统的核心理念。

如果所有节点都有真实身份的话，那么设计上会更加容易。有了真实身份，我们就能够以这样的方式发出协议指令，比如“编号最小的节点开始做某些动作”，在没有真实身份前提下，系统能设计的指令就受到很多限制，但设计真实身份最主要的考虑是安全上的便利。如果节点的身份可以被识别，就不能随便地制造新的节点身份出来。那样的话，我们就可以假设有恶意节点的数量，然后部署安全措施来防范。基于以上原因，缺少真实身份给比特币的共识协议带来很多难点。

我们可以做一个较弱的理论假设来弥补这个先天的不足。假设我们可以在系统里随意选一个节点，一个比较好的比喻是——就如同在彩票站，或是在任何一个难以辨别每个人身份的系统中，我们给每一位顾客发出彩票或是一个识别牌，之后我们就可以开始抽奖，与奖号对应的人就会中奖。现在我们想象一下在比特币的世界里，我们假设也可以做到

这一点。我们再假设，这个彩票的印制过程与发放办法是足够聪明的，如果一个黑客想制造出许多女巫节点来，最后所有这些节点也只能拿到一张彩票。也就是说，这个黑客无法通过制造假的节点来增强他的力量。如果你觉得我们做的假设太多了，请不要担心，我们在以后会消除这些假设，并在后文会详细说明，在比特币系统中，与这些假设相对应的性质是如何实现的。

隐性共识

对随意节点选择的假设可以让“隐性共识”（implicit consensus）成为可能。我们的共识协议有多个回合，每个回合都对应着区块链里的一个块。在每一个回合里，一个随机节点会被选中，然后这个节点可以提议这个链的下一个区块。这时没有共识算法，也没有任何投票过程来决定哪个区块会被选中，随机被选中的节点会直接决定区块链的下一个区块，但万一这个节点是恶意的呢？针对这个问题，还是有应对办法的，解决方法就是隐性共识。其他节点可以通过隐性地接受或是拒绝前面这个被随机选择出来的节点。如果接受，它们会在这个块之后接龙下去；如果拒绝，它们忽略这个新的区块，而是选择前一曾经接受的区块，来继续接龙下去。大家还记得，每一块都记录着前一块的哈希值。这就是节点选择在哪一块来继续接龙的技术处理方式：比特币共识算法（简化版）。

这个算法的简化假设是，可以随意选择一个节点，这些节点都不会受到女巫攻击的影响。

1. 新的交易被广播到所有节点上。
2. 每个节点都将新的交易放进一个区块。
3. 在每个回合，一个随机的节点可以广播它的区块。

4. 其他节点可以选择接受这个区块，前提是如果区块里的交易都是正当的（有真的签名）。

5. 节点们可以把以上区块的哈希值放进自己的区块里，以此来表示它们对那个新区块的认可。

我们现在一起来研究一下为什么这样一个共识算法是有效的。为此，我们假设有一个叫爱丽丝的黑客，她想要破坏这个共识过程。

窃取比特币

爱丽丝能够窃取属于另一个用户，不受她控制的地址里的比特币吗？答案是否定的。即使这一轮是由爱丽丝提议区块链上的下一个区块，她也不可能窃取别人的比特币。这么做的话，爱丽丝需要发起一笔有效的交易来花掉这个比特币。这就要求爱丽丝伪造比特币拥有者的签名，然而如果数字签名机制是安全的，她是无法办到的。只要背后的密码学基础是牢靠的，她就无法轻易窃取比特币。

拒绝服务攻击

让我们来考虑另一种攻击。假设爱丽丝不喜欢叫鲍勃的某个用户，爱丽丝可以决定她不把鲍勃发起的任何交易放进她所提议的区块里。换言之，她拒绝提供服务给鲍勃。尽管这是爱丽丝可以开展的有效的攻击，但幸好这不过是个小问题。如果鲍勃的交易没有被放进爱丽丝所提议的下一个区块，鲍勃只要等到下一个诚实节点发起区块的时候，他的交易记录就会被放进这个区块里。所以这其实也不算是一个有效的攻击。

双重支付攻击

爱丽丝也可能会发起一个双重支付攻击。要理解爱丽丝如何发起这

种攻击，我们可以假设爱丽丝是鲍勃开的网店或网站的一名顾客。鲍勃提供一些比特币付费的在线服务，比如软件下载。双重支付攻击是这样的：爱丽丝在鲍勃的网站选中一件商品并加入购物车中，此时服务器要求付款。然后，爱丽丝在她的地址上向鲍勃的地址发起了一笔比特币交易，并向整个网络广播这笔交易。我们假设由某个诚实节点来制造下一个区块，并把这笔交易放进这个区块中。因此，现在就有了一个由诚实节点发起，包含代表爱丽丝向商家鲍勃支付这笔交易在内的区块了。

我们还记得一个交易就是一个数据结构，里面有爱丽丝的数字签名，一个付给鲍勃的公钥（地址）的指令和一个哈希值。这个哈希值代表了一个指针，指向先前的一笔交易的输出，即爱丽丝之前收到并于现在消费比特币。这个指针必须指向一个已被共识链上的某个之前的区块所认可的交易。

顺便说一下，有两种容易混淆的不同类型的哈希指针。一种是在区块内用来表示接在之前哪个区块后面的哈希指针；另一种是在交易里的一个或多个，用来指向之前交易里说明比特币来源的哈希指针。

我们回到爱丽丝如何发起双重支付攻击这个问题。最新的一个区块由一个诚实节点产生，其中包含爱丽丝下载软件向鲍勃付费的交易记录。当看到这笔交易被放入区块链后，鲍勃认为爱丽丝已经向他付款，便允许爱丽丝下载软件。假设在下一个回合被随机选中的节点恰巧被爱丽丝所控制。现在因为爱丽丝可以提议下一个区块，她可以选择忽略掉前面那个包含她支付给鲍勃的那笔交易的区块，而产生一个包含指向之前区块指针的区块。不仅这样，在这个区块里，爱丽丝可以放进一笔交易，把她付给鲍勃的币转到一个被她所控制地址里去。这就是一个经典的双重支付攻击。因为这两个交易用的是同一个币，只有一个交易可以被放进区块链。所以如果爱丽丝成功地把币转到她控制的地址，那个她付币给鲍勃的交易记录将变得无效，因为它将不会被放进区块链里。这一过程详见图2.2。

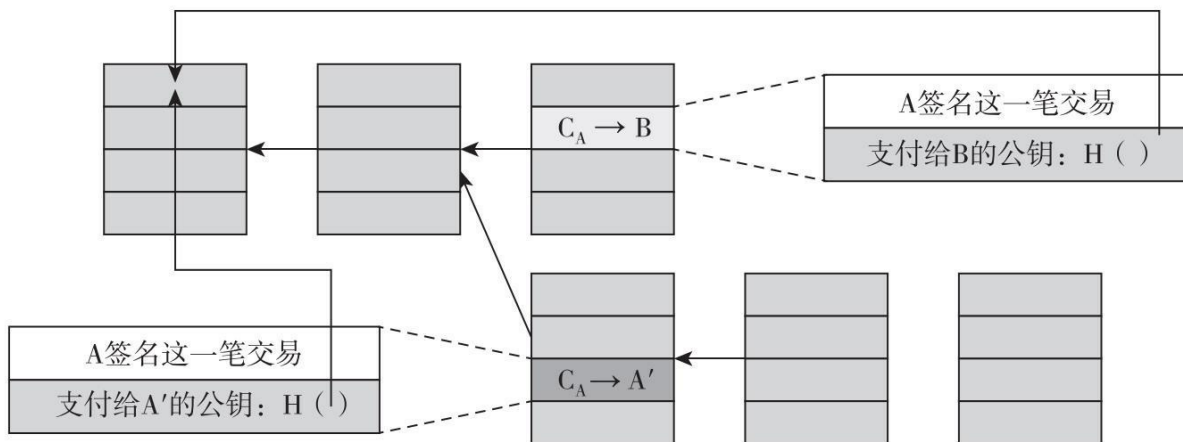


图2.2 双重支付攻击

注：爱丽丝创建了两笔交易：一笔是她付给鲍勃比特币的交易，另一笔是她将这笔比特币重复支付到她控制的另一个地址。因为这两笔交易用相同的比特币支付，所以只有一笔会被放进区块链。图中的箭头表示一个区块链接到前一个区块的指针，通过在前一个区块自己的内容中包含了一个哈希值进行了扩展。 C_A 代表爱丽丝拥有的币。

那我们如何知道这个双重支付攻击是否能成功呢？这取决于最后哪个区块会被纳入长期的共识链，是爱丽丝转给鲍勃的区块，还是爱丽丝转给爱丽丝自己的区块。是什么决定了哪一个区块被纳入呢？诚实节点会遵守在最长有效分支后面延展这一规则，那到底在哪个分支后面延展呢？并没有明确的答案！目前来看，这两条分支长度一样，它们的区别是仅在于最后一个区块，并且这两个区块都是有效的。选择下一个区块的节点可以决定建立在其中一个区块上。这个选择就决定了双重支付攻击的成功与否。

微妙之处在于：从道德角度考虑，这两个分支截然不同，一个是包含付给鲍勃交易的区块，一个是包含爱丽丝把这些币双重支付给她自己地址交易的区块。但这个区别仅仅建立在我们知道爱丽丝先支付给鲍勃再试图双重支付这个故事的基础上。但从技术角度来看，这两笔交易完全一致，且都有效。节点没有办法分辨出哪一个是在道义上合理合法的交易。

实践中，节点往往用延展它们在点对点网络里最早听到的区块这种

启发式的方法。但这不是一个无懈可击的法则。在一些情况下，因为网络延迟，很可能它们先听到的区块实际上是后被创造出来的。所以下一个提议节点至少是有可能选择在那个包含双重支付的区块上延展。爱丽丝甚至还可以贿赂下一个提议节点来加大这个可能性。不管出于什么原因，如果下一个节点真的接受了这个双重支付的区块，那么这条链将比包含支付给鲍勃交易的那条链更长。基于此，下一个诚实节点就有可能去延展这条链，因为它更长。随着这个过程继续，这条包含双重支付的链会更有可能成为长期共识链的一部分。相反，那个包含爱丽丝支付给鲍勃交易区块的链会被网络完全遗忘，成为一个**孤块**（orphan block）。

我们现在从商家鲍勃的立场重新考虑整个情况。理解鲍勃如何保护自己不受双重支付攻击是理解比特币安全措施的重要的一部分。当爱丽丝广播她向鲍勃支付的交易时，鲍勃也在网上听着，鲍勃在下一区块被创建之前就能听到这笔交易。如果鲍勃比我们前面描述的更加草率的话，他可以在网上完成检查程序，并允许爱丽丝此时下载软件。这叫作**零验证交易**(zero confirmation transaction)。这将导致一个比前面所说的更加基础的双重支付攻击。前面所述情况，为了实现双重支付攻击，我们需要假设一个恶意黑客控制了发起下一个区块的节点。但如果鲍勃允许爱丽丝在没有收到区块链一条确认信息的情况下就下载软件，那么爱丽丝可以立刻广播一条双重支付交易，一个诚实节点就有可能把这个交易放进下一区块，而不是支付给鲍勃的那笔交易。见图2.3。

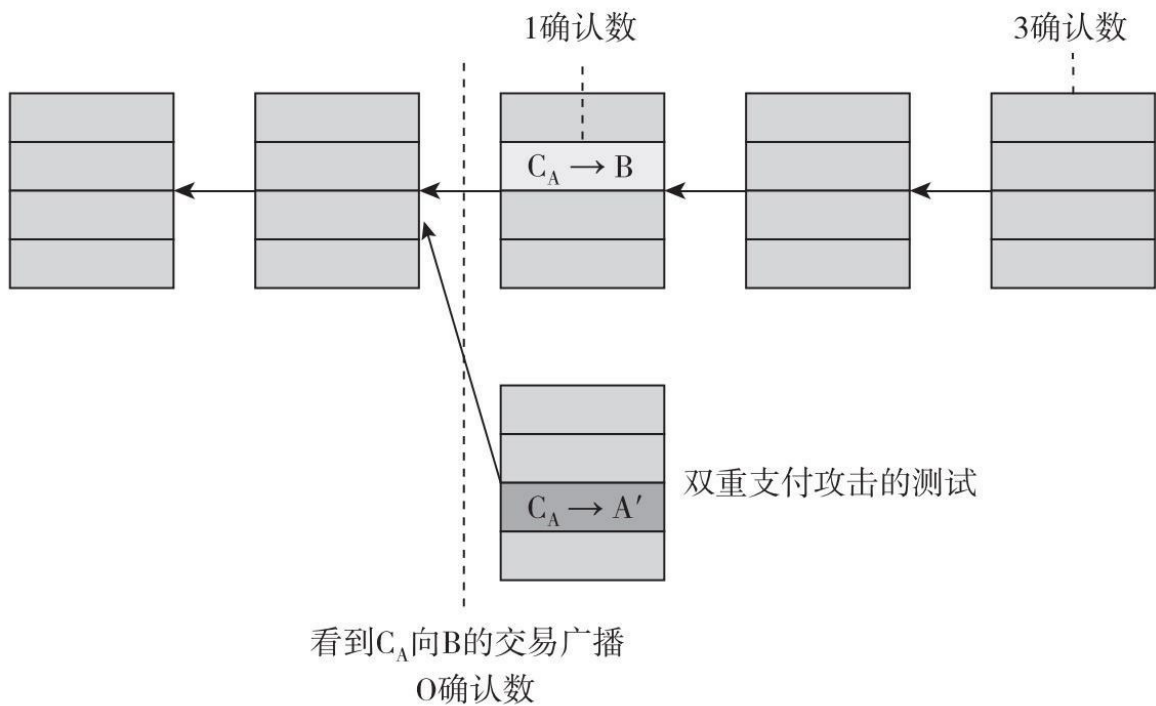


图2.3 从鲍勃立场来看双重支付

注：这是一个从商家鲍勃的立场来看爱丽丝做的双重支付尝试。为了保护自己免受双重支付攻击，鲍勃应当等爱丽丝向他支付的交易被区块链包含进去，并且多等几次确认。

另一方面，一个谨慎的商家甚至在看到交易被包含在一个区块后仍然不会允许爱丽丝下载软件，而是继续等待。如果鲍勃看到爱丽丝成功发起了双重支付的攻击，他会意识到那个含有爱丽丝向他支付的交易的区块有可能已经被丢弃。他应该放弃这个交易，不让爱丽丝下载软件。如果在尝试双重支付的情况下，恰巧下几个节点还是建立在爱丽丝向鲍勃支付交易的区块上，那鲍勃就相信这笔交易会被纳入长期共识链。

总而言之，一个交易得到的确认越多，它被纳入长期共识链的概率就越大。如前文所述，诚实节点总是选择延展最长的共识链。因为长链增长更多，那条含有双重支付的短链追上长链的概率会变得越来越小。在只有一小撮恶意节点的情况下，这个结论尤其正确。因为短链要想赶上，这些恶意节点需要被一直连续选中。

事实证明，双重支付攻击成功的概率将随着确认的数目的增加而指

数级降低。所以，如果你感兴趣的交易已经收到 k 个确认，双重支付攻击交易被纳入长期共识链的概率以关于 k 的一个函数指数级下降。在比特币生态系统里，最常见的方法是等6个确认。并不是6这个数字有什么特殊意义，只不过，这样在你等待的时间与确认你所感兴趣的交易被纳入长期共识链之间做了很好的平衡^[1]。

总结起来，防止不正当交易完全是用密码学的方法。但这些方法被共识所加强，意思是一个节点如果想放进一个密码学上不正当的交易，这个交易不会被纳入长期共识链的唯一原因是绝大多数的节点是诚实的，不会把一个不正当交易放进区块链。另外，防止双重支付攻击完全依赖于共识，密码学不起任何作用。从密码角度来看，这两个交易都是正当有效的。但共识可以决定哪个被放进长期共识链。最后，你无法百分之百保证你感兴趣的交易被放进了长期共识链。但指数级概率保证了不错的结果，6笔交易过后，实质上你没有犯错的可能了。

^[1] 如后文总结时所说，并没有一个固定的数字，但6是个常用的数目。——译者注

2.4 奖励机制与工作量证明

在前面的章节里，我们简单了解了比特币的共识算法，以及为什么我们直觉上相信它是安全的。但我们回想在本章一开始谈到的，比特币的去中心化一部分是通过技术手段，另一部分是通过聪明的激励设计来实现的。截至目前，我们主要关注的还是技术手段。现在，我们来讨论比特币的这个激励设计。

之前我们试图大胆相信这样的假设，在我们随机选取节点时，至少有50%的可能会选中诚实节点，这或许是有问题的。如果对颠覆这个过程的参与者有金钱奖励，这个关于诚实的假设就格外成问题，这种情况下我们无法真的假设某个节点是诚实的。所以这个问题变成了：我们是否可以给予表现诚实的节点奖励？

我们再思考下一个确认以后的双重支付尝试（见图2.3）。我们是否可以惩罚那个创建包含双重支付区块的节点？好吧，其实不行。就像我们前面说的，因为我们无法判断哪笔交易是道义上合法的。即使我们知道，我们也很难惩罚它们，因为节点没有身份。那我们反过来思考，我们是否可以奖励那些创造的区块最终被放入长期共识区块的节点？然而，同样因为这些节点并没有透露它们真实世界中的身份，我们不可能给他们的家庭地址寄去现金。要是有一种可以代替的数字货币……你大概猜到该怎么做的。我们可以用比特币来奖励创造这些区块的节点。

让我们暂停一下。之前，我们讨论的都是用抽象的算法来实现分布式共识，并不是针对某个具体的应用。我们现在要跳出模型，使用事实，我们建立这个分布式共识过程的应用实际上就是一种货币。明确地说，我们要以这种货币为单位奖励那些表现诚实的节点。

区块奖励

这是怎么做到的？比特币里有两种不同的奖励机制。其中一个就是区块奖励。根据比特币的规则，创建区块的节点可以在这个区块中加入一笔特别的交易。这笔交易就是一个造币的交易，类似于财奴币里面的造币，节点可以指定这笔交易的接收地址。当然，节点通常都会选择一个属于自己的地址。你可以把这视为对节点在共识链上进行创建区块服务的报酬。

在写本书时，区块奖励金额定在25个比特币。但每生成210 000个区块，金额就会减半。根据区块生成的速度，我们可以看到，这个金额大概每4年减半一次。我们现在处在第二个4年。比特币存在的最初4年，区块奖励金额为50个比特币，现在是25个比特币。然后会不断减半。这将造成一些有意思的结果，我们不久会看到。

你可能会问为什么区块奖励能做到鼓励诚实行为。给予我们目前讨论的，从表面上看，这个节点无论提议一个正当有效的区块还是恶意伪造，都会受到奖励。但其实并非如此！想一想这个节点是如何收取奖励的？奖励只有当区块最终被纳入长期共识链才会实现。因为造币交易和其他每一笔交易一样，只有当它最终被纳入共识链，才会被其他节点接受。这就是比特币奖励制度的一个关键概念。这是一个十分微妙却十分强大的设计。这个设计激励节点想方设法让其他节点延展它们自己的区块。因此如果网络中大部分节点遵循去延展最长支链的规则，那这样的设计将激励所有节点去遵循这个规则。这就是比特币的第一个奖励机制。

我们前面提到每产生210 000个区块（大约4年），区块奖励将被减半。在图2.4中，曲线的斜率将持续减半。这是一个等比数列，你可能知道数列的总和是有上限的。最终一共是21 000 000个比特币。

注意，这是新比特币被允许创造出来的唯一途径，没有任何其他新增币的机制。所以这是为什么比特币最终的数量是2 100万（至少目前的规则规定是这样）。按照现在奖励发放的速度，到了2140年比特币区块奖励就发完了。这是否意味着这个系统到了2140年就无法继续运行，并且因为不再有奖励诚实行为的激励而变得不安全呢？不是这样的。因为区块奖励只是比特币两种奖励机制之一。

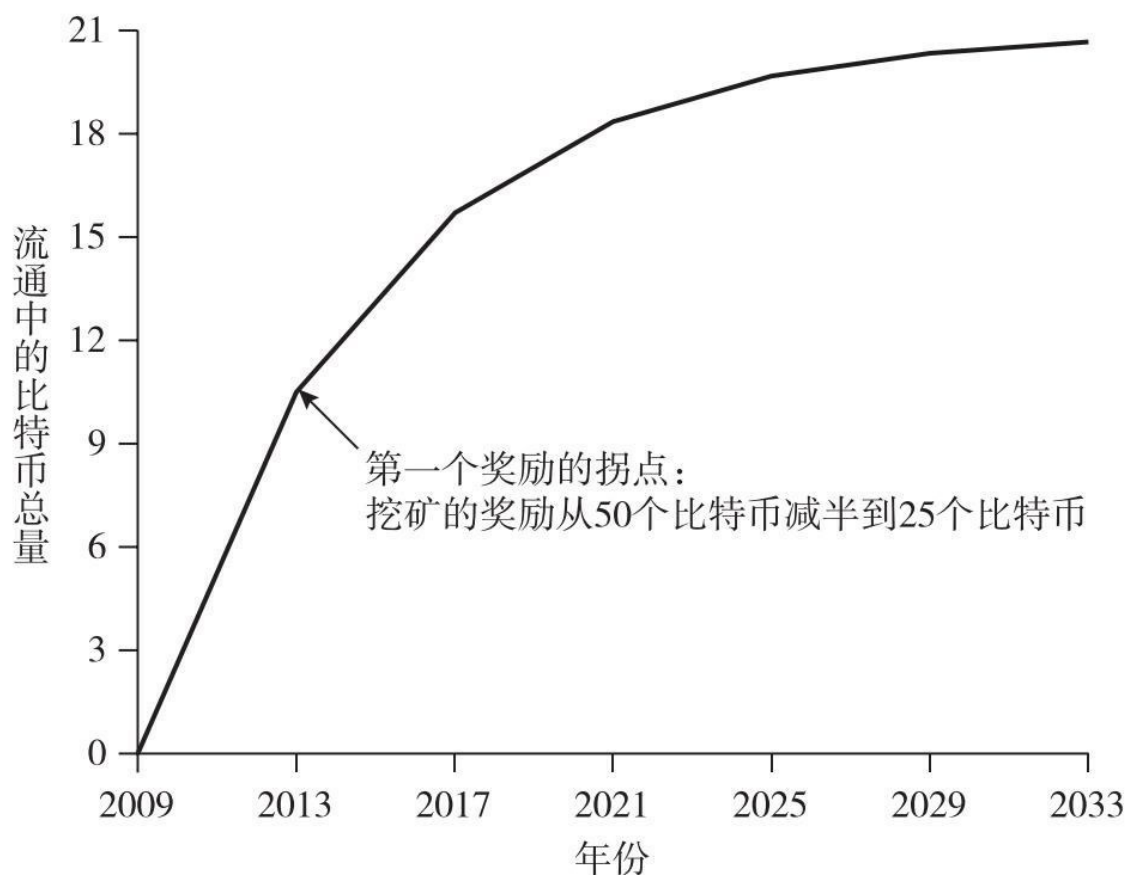


图2.4 比特币的总供应量

注：区块奖励每4年减半一次，限制了比特币的供应上限为2 100万个。这是一个简化的模型，实际中的曲线会有轻微的差异，但都有2 100万的上限限制。

交易费

比特币的第二个奖励机制称为交易费。任何交易的制造者都可以选择让交易输出值比输入值小。第一个创建区块把交易放进区块链的人可以取得这个差额，作为交易费。如果你是一个节点，正在创建一个包含200笔交易的区块，那么这200笔交易的交易费将会被付到你放在区块内的那个地址。这些交易费现在是完全自愿的，但是我们可以预见，随着区块奖励逐渐发完，交易费会变得越来越重要，几乎是必需的，因为用户需要通过交易费来保障合理的服务质量。从某种程度上来说，这已经开始发生。但目前还不清楚这个系统会如何演变——这取决于还并不完善的博弈论的研究与发展。这也是比特币一个很有趣的研究领域。

我们在描述共识机制时还有一些问题没有解答。第一个主要问题是我们要你相信这样的假设：我们能随机选取一个节点。第二个是因奖励那些节点参与而产生的新问题：如果大家都想来分一杯羹成为一个节点来获得这些奖励的话，整个系统会变得不稳定。第三个是第二个问题的复杂版，就是可能会有攻击者创建大量的女巫节点来尝试颠覆整个共识过程。

挖矿与工作量证明

事实证明，这些问题都是相互联系的，所有这些问题都有相同的解决办法——**工作量证明**（proof of work）。工作量证明的核心理念是，我们把随机选取节点改为根据节点占有某种资源的比例来选取节点，我们希望这种资源是没有人可以垄断的。比如说，如果这个资源是计算能力，那我们称之为工作量证明系统。或者这个资源可以是某种币的拥有量，我们称之为**权益证明**（proof of stake）。虽然比特币没有使用，但权益证明也是另一种合格的模式，并被其他加密货币所使用。我们将在第8章中更多地讨论权益证明和其他工作量证明的变种。

先回到工作量证明。我们试着更好地理解根据计算能力来选择节点

到底是什么意思。换一个角度理解，我们是允许节点用它们的计算能力来互相竞争，导致的结果是计算能力的比例决定了节点被自动选中的概率。工作量证明还有一种理解方式，即我们把制造新身份的难度适度提高了。这就好像是对制造新身份，继而对女巫攻击收税一样。这听起来好像有点模糊，我们接下来看下比特币使用时工作量证明体系的细节，事情就变得清楚多了。

比特币是用哈希函数解谜来证明工作量的。任何一个提议并创建区块的节点想要制造下一块，这个节点必须要找到一个数，或者我们把它称为临时随机数（见第1章1.1节）。当你把这个临时随机数、前序块的哈希值还有要填进这个区块的交易列表连接起来，组成一整串字符，然后用哈希函数计算这一整串字符的输出值，这个输出值正好要落在一个相对于这个哈希函数所有可能的输出中很小的目标区间内。用公式来表示的话，就是临时随机数要满足下面的不等式：

$$H(\text{nonce}||\text{prev_hash}||\text{tx}||\text{tx}||\dots||\text{tx}) < \text{target}$$

就像我们前面看到的，通常一个区块会包含这个节点提议的一系列交易。而且，这个区块还会包含一个指向前序区块的哈希指针（我们这里说的哈希指针是一个宽泛的概念。这个指针只是文本中的字符串，它并不需要告诉我们去哪里找到这个区块。我们可以通过在网上询问其他的节点找到区块。重要的是，这个哈希值既作为我们在网络上请求其他节点寻找区块的ID，又能够让获取这个区块后验证它）。除此之外，我们现在还要求区块包含一个临时随机数。这个想法是为了适度提高发现符合要求的临时随机数的难度，即把包含临时随机数在内的整个区块的哈希值组合到一起，输出结果要是一种特定的形式。如果哈希函数符合我们在第1章中所描述的谜题友好特性，那唯一解出哈希谜题的办法就是去试足够多的临时随机数，直到成功为止。具体来说，如果这个目标区域是所有可能的输出的1%，那你大概就要试100次才能成功。事实上，这个目标区域远比输出范围的1%小得多得多，我们后面就能看

到。[\[1\]](#)

用这种哈希函数解谜以及工作量证明的办法，我们可以完全舍弃采取那种随机选取节点的办法。这些节点在竞争哈希函数解谜的过程中一直都是互相独立的。有时一个节点鸿运当头，正好发现一个临时随机数可以满足要求。这个幸运的节点就可以提议创建下一个区块了。这就是比特币系统实现完全去中心化的方式，没有任何人能决定谁可以提交下一区块。

难于计算

哈希谜题有三个重要的特性。第一个特性是要有一定的难度。我们前面说适度的难度，其实你马上会看到难度实际上是随时间而改变的。在2014年年底，产生一个区块平均要做 10^{20} 次哈希运算。换言之，目标区域仅仅是整个输出范围的 $1/10^{20}$ 。这是超大的计算量——举例来说，超过了商业化笔记本电脑可能的计算范畴。因此，只有一些节点还在不厌其烦地竞争造块。这个不停尝试解哈希谜题的过程，就是我们听说的比特币挖矿，参与挖矿的节点被称为矿工。尽管技术上每个人都可以成为矿工，但由于挖矿的高成本导致了挖矿生态系统要消耗大量能源。

可参数化成本

第二个特性是，我们希望成本是可以通过参数来变化的，而不是一个固定值。在比特币的点对点网络里，是这样来达到这一特性的：每产生2 016个区块之后，所有的节点都会自动重新计算目标区域相对于整个输出范围的比例大小，使得后续的区块产生的时间间隔约为10分钟。两个区块之间的平均间隔是10分钟，2 016个区块就需要两个星期。所

以大约每两个星期，目标区域的大小会被重新计算一次。

我们想一下这意味着什么。如果你是个矿工，你花了一定的费用投资了一些硬件来做比特币挖矿。但是整个挖矿体系在不断增加，越来越多的矿工加入这个行业，或是他们部署了运算越来越快的硬件设备，那两个星期的时间段里，被找到的区块可能比预期的要多一点。然后，那些节点就会自动调整目标区域，你要找到一个块所要做的工作量就随之增加。所以如果你投了一笔固定资金在硬件上，你找到下一区块的速率实际上取决于其他矿工在做什么。有一个公式可以很好地描述这一点：任何一个矿工，比如爱丽丝，找到下一区块的概率，就相当于她控制的计算力占整个全球计算力的比例。这意味着，如果爱丽丝的挖矿设备的计算能力占全部计算能力的0.1%，那大概每产生1 000个区块，她就可以找到一个区块。

这样重新调整的目的是什么？我们为什么想要维持10分钟间隔不变？原因很简单。如果区块产生的间隔太小，就会造成很多低效率，我们还会失去许多优化上的好处，比如在一个区块内放入大量的交易。10分钟并没有神奇之处，如果把10分钟下调到5分钟大概也可以。关于其他加密货币的理想区块间隔应该是多少，已经有很多讨论。除去关于理想间隔的不同意见，大家都认为应该是个固定的值。它不允许被无限降低。这就是为什么我们有自动重新计算目标区域的特征。

这个成本函数和工作量证明的设定方式，让我们重新审视比特币的安全假设。现在我们终于可以丢弃之前让你盲目相信的假设。不必再去说那些连身份都没有的节点大多数是诚实的了，诚实具体代表什么也并不清楚，我们现在可以清楚地表述，只要以计算能力为权重的大多数矿工，遵循比特币协议，或者说是诚实的，那么比特币中的大量攻击就都没有可能发生。因为如果以计算能力为权重的大多数矿工是诚实的，提议下一个区块的竞争会自动保证在任意时间点，下一个区块至少有50%的概率是由一个诚实节点提议的。



矿工行为的两种行为模式

在分布式系统和计算安全研究领域，假设一定比例的节点是诚实的，来展示在其他节点表现随意的情况下，系统如何按照预期运行，是很常见的方法。这是我们采用的基础方法，除了以计算能力为权重计算大多数之外。最初的比特币白皮书也包含了这样的分析。

但博弈论领域给出了一种完全不同的，更复杂且实际的方法来决定系统如何运行。这个观点不区分节点诚实或恶意，而是假设每个节点都按自己的意愿行动。每个节点考虑其他节点的潜在可能策略之后，采用一种（随机的）策略最大化自己的回报。如果协议和激励机制设计得当，大多数节点在大多数时候会遵循这个规则。“诚实”的行为只是许多策略中的一种，我们在道德上并不依赖于此。

博弈论的观点认为，最大的问题是矿工默认的行为是否是一种“纳什均衡”（Nash equilibrium），即这是否代表了一种稳定的状态，在这种状态下没有节点可以通过表现不诚实而获得更高的回报。针对这个问题现在各界仍有争议，并且是一个活跃的研究领域。

解哈希谜题是概率性的，因为没有人可以预测到哪个临时随机数会解出谜题。唯一的方法是一个一个去试临时随机数，并希望能够成功。在数学上，这被称为伯努利试验（Bernoulli trial）。伯努利试验是一种有两种可能结果的试验，在连续试验下，每种结果发生的概率是固定的。在这里，两种结果是哈希值是否落在目标区域内，假设哈希函数像随机函数一样，那些结果的概率都是固定的。典型地，节点多次尝试临时随机数的伯努利试验是一个离散概率过程，它可以用一个叫作泊松过

程（Poisson process）的连续概率过程近似表示，在泊松过程中，事件以固定的速率独立出现。最后的结果是，发现下一个区块所需要时间的概率密度函数，见图2.5。

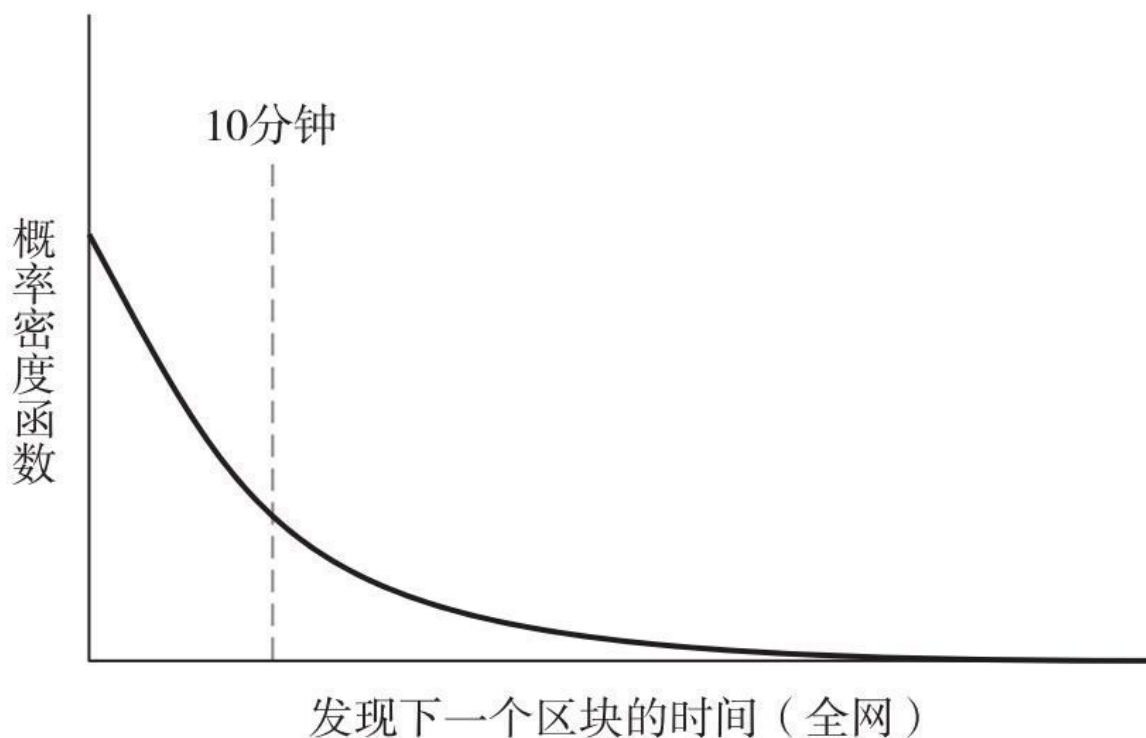


图2.5 发现下一个区块所需时间的概率密度函数

这被称为指数分布。假设一个区块现在被发行，下一个区块有一定的小概率很快被发现，比如几秒钟或几分钟。也有一定的小概率花了较长时间才发现下一个区块，比如一小时。但总体来说，网络会自动调整难度使得区块间隔时间的长期均值维持在10分钟。注意图2.5表示的是整个网络内区块被创造出来的频率，而不是哪个矿工事实上发现了这个区块。

如果你是一名矿工，你大概想知道要多长时间才能找到下一区块？这个概率密度函数会是什么样？它的形状会相同，但x轴的坐标不一样。可以用一个漂亮的公式表示：

对于某个特定的矿工：

发现下一区块的平均时间=10分钟/占全部计算能力的比例

如果你有全网络0.1%的计算能力，这个公式告诉我们，你每10 000分钟能找到一个区块，大约一个星期。不仅是你发现区块的时间间隔非常长，时间间隔的波动也会非常大。因此产生的一些重要结论我们在第5章会讲到。

易于证实

现在回到工作量证明函数第三个重要的特性，就是证实一个节点正确地计算了工作量证明很容易。即使一个节点要尝试 10^{20} 次来找到使区块哈希值落在目标范围内的临时随机数，并且临时随机数必须是作为区块的一部分被公布出来。这样任何其他节点很容易检查区块的内容，计算它的哈希值，证实它的输出在目标区域内。这是个相当重要的特征，因为这样使得我们摆脱了中心化管理。我们不需要一个中央权威机构来证明矿工正确地完成了工作。任何节点或者矿工，都可以迅速地证实其他矿工找到的区块符合工作量证明的规定。

[1] 这段话很拗口，也难懂。打个比方，假如你是个炮兵，那些前序区块哈希值加上所有要打包的交易就是炮弹，哈希函数就是大炮，临时随机数就好比瞄准器，你所想击中的目标，比如一个指挥所，它肯定在你能打到的范围内，但非常小，而且其实根本不知道在哪里。击中目标的唯一办法是狂轰滥炸，这就是比特币工作量的概念，炸的越多，击中的概率越高。如果这个指挥所的目标区域是轰击区域1%大的话，你大概平均要发出100枚炮弹才可能击中目标。

——译者注

2.5 总结

挖矿成本

我们现在来看一下挖矿经济学。前文提到过，作为矿工挖矿是十分昂贵的。按现在的难度，找到下一个单独的区块需要计算 10^{20} 个哈希值，区块奖励约是25个比特币，按照现在的比特币汇率，是不小的一笔钱。这些数据可以让我们简单地计算出挖矿是否赚钱。我们可以用这个简单的逻辑来做这个决定：

如果：

挖矿奖励 > 挖矿成本

那么：

矿工赚钱

条件是：

挖矿奖励 = 区块奖励 + 交易费

挖矿成本 = 硬件成本 + 运营成本（电费、空调费等）

基本上，矿工的挖矿奖励就是区块奖励和交易费。矿工自己与总的支出相比较，包括硬件和电费成本。

但这个简单的公式也有几个复杂的地方：第一，硬件投资是固定的，但电费是个变量，随时间变化。第二个复杂之处是，矿工得到的奖励取决于他们发现区块的速度，这不仅取决于他们硬件的能力，还取决

于他们的计算能力占全球计算能力的比例。第三是挖矿产生的成本通常是用美元和其他传统货币表示的，但他们得到的奖励是比特币。所以这个方程在任何时候都有一个隐藏的因素，就是比特币的汇率。第四，到目前为止，我们都假设矿工会诚实地遵守协议。但矿工有可能选择用一些其他的挖矿策略，而不总是试图延展最长的有效分支。所以这个方程没有囊括所有矿工可以用到的不同策略的细微差别。事实上，要想分析挖矿是否有意义，是一个博弈论问题，没有那么容易找到答案。

到此为止，我们已经较好地理解了比特币如何实现去中心化。我们现在总结一些关键点，放在一起以便更好地理解。

我们首先从身份开始。根据我们知道的，比特币协议不需要真实世界的身份就可以参与。任何用户任何时刻都可以制造一对匿名的钥匙。如果爱丽丝想付给鲍勃比特币，比特币协议里没有详细说明爱丽丝如何得知鲍勃的地址。在这些匿名的钥匙对用作身份的情况下，交易其实是向整个点对点网络广播的信息，把比特币从一个地址转到另一个地址。比特币只是交易输出，我们在下一章节会深入讨论这个问题。



不存在所谓“1比特币”这样的东西

比特币没有固定面额，不像美元。具体来说，没有“1比特币”这样的特别名称。比特币只不过是交易输出，在现在的规则里，它们可以是精确到小数点后8位的任意值。可能的最小价值是0.000 000 01 BTC（比特币），我们称之为1个中本聪（比特币的发明人）。

比特币点对点网络的目标，是把所有新的交易与新的区块传播到所有比特币节点。但这个网络很不完美，只能尽其所能来传递信息。这个系统的安全性不是来自点对点网络的完美，而是来自我们本章中重点讨

论的区块链和共识协议。

当我们说一个交易被放进了区块链，我们真实的意思是这笔交易已被确认了许多次。对于多少次确认足以让我们确信交易已包含在内，并没有一个固定的数字，但6次是个常用的数目。一笔交易收到的确认越多，你就越可以确信这笔交易被放进了区块链。经常会有一些孤块，或者没有进入共识链的区块。有很多原因可以导致一个区块变为孤块。这个区块可能包含一个不正当交易，或者试图双重支付。也有可能是网络延迟，这里指的是，两个矿工可能相隔几秒找到了新的区块，这两块几乎同时被广播到网上，那其中一块肯定会被丢弃。

最后我们看了哈希谜题与挖矿。矿工是决定参与创造新区块竞争的特殊类型节点。如果其他矿工继续在他们的区块上搭建的话，对于他们努力的回报是新造的比特币（新区块奖励）和已经存在的比特币（交易费）。很微妙也很重要的一点是：假设爱丽丝比鲍勃的计算能力要强大100倍，但这并不意味着爱丽丝一定能够赢得找到下一区块的竞赛，而是爱丽丝和鲍勃发现新区块的概率比率是100：1。长期下来，鲍勃找到的区块数量是爱丽丝的1/100。

我们预计矿工们会处在经济平衡点附近，意味着他们得到的奖励大致等于他们在硬件与电费上的花费。理由是如果一个矿工持续亏钱，他会停止挖矿。反之，如果硬件和电费固定的情况下，挖矿利润很高，那更多的挖矿设备会加入网络。计算能力的增加会导致难度提高，每个矿工预期的回报便会降低。

比特币深度使用了分布式共识的概念。在传统货币系统中，共识的作用是有限的。具体来说，有一个共识过程来决定货币的汇率。这在比特币里当然也是对的——我们需要围绕比特币价值的共识。但在比特币里，我们还需要对账本情况的共识，这是由区块链来完成的。换句话说，甚至你拥有多少比特币的算法都是依赖共识的。当我们说爱丽丝拥有一定数量的比特币，我们真实的意思是说在比特币点对点网络，在区

区块链中记录的所有爱丽丝地址上拥有的比特币数量总额。这是比特币系统的一个终极真相：拥有比特币就是其他节点对给定的一方拥有这些比特币的共识。

最后，我们必须对整个系统的规则达成共识，系统规则有时不得不改变。比特币规则改变有两种：对应为软分叉与硬分叉。我们把关于它们区别的详细讨论放到第3章和第7章中。

启动加密货币

另一个微妙的概念是“自举过程”（bootstrapping）。比特币系统里三个不同的想法——区块链的安全性、挖矿生态系统的健康程度，以及货币的价值在相互作用。我们显然希望区块链安全，这样比特币才能成为一种可行的货币。想要区块链安全，就要保证黑客不能倾覆共识过程。这反过来意味着，一个黑客不能够制造一大堆挖矿节点来占据50%以上的新区块生成。

但如何实现这一点呢？前提条件是有一个健康的挖矿生态系统，其中大部分节点是诚实的、遵守协议的。但健康的挖矿生态系统的前提条件又是什么呢——我们什么时候可以保证大多数矿工会把大多数计算能力运用到解哈希谜题的竞争中呢？好吧，只有在比特币价位高时他们才会这么做，因为他们收到的奖励是比特币而他们的花费都是美元。所以币的价值越高，矿工就越有动力这么做。

那如何保障币的价值又高又稳定呢？只有用户普遍相信区块链的安全性才会发生。如果他们认为网络随时会被攻击者颠覆，那比特币作为货币将一文不值。所以你可以看到区块链的安全性、挖矿生态系统的健康程度和货币的价值这三者之间相互依赖、相互作用的关系。

因为这三者之间的循环依赖关系，其中一个的存在可以用另一个的

存在推测出来。在比特币初创之时，这三者都不存在。除了中本聪自己，没有人在运行挖矿软件。比特币作为货币没有什么价值。事实上，因为没有很多人挖矿，区块链也很不安全，任何人都可以轻易颠覆这个过程。

这三者在比特币的世界如何从无到有并没有一个简单的解释。媒体的关注是其中一个因素——听到比特币的人越多，感兴趣挖矿的人就越多。挖矿的人越多，人们就会对区块链的安全越有信心，因为更多挖矿活动在进行，以此类推。附带提下，每种其他虚拟货币想要成功也需要想办法通过自举过程解决这个问题。

51%攻击

我们考虑一下如果共识失败，并且存在一个在比特币网络里实际掌握了绝大部分挖矿计算能力的51%攻击者，会发生什么情况。我们考虑多种可能的攻击，分析哪些可能被这样的攻击者实际使用。

首先，攻击者可以从现存的地址里偷币吗？你可能猜到了，不行，因为除非你能推翻加密方法，否则从现存地址偷币是不可能的。它不足以颠覆共识过程。这样说还不是很清楚。我们不妨假设，51%攻击者制造了一个不正当的区块，里面有一笔不正当交易把币从不受其控制的地址转移到自己的地址。攻击者可以假装这是一笔正当的交易，继续在这个区块上建造，甚至可以把它变成一个最长的支链。但其他诚实节点不会简单地接受这个存在不正当交易的区块，它们还是会在网络中找到之前最后一个正当的区块，基于此继续挖矿。所以将会发生的是，链上出现了我们称之为分叉的情况。

现在想象一下这个攻击者想把这些非法的币花掉，付给某个商家鲍勃用来买他的商品或者服务。鲍勃可以假定运行着自己的比特币节点，

而且是一个诚实节点。那鲍勃的节点会因为含有不正当的交易而拒绝这个非法的分支。因为那里面的数字签名不吻合。所以鲍勃的节点会忽略这个最长的支链，因为这是一个非法的支链。而因此，这不足以颠覆共识。你需要推翻加密方法偷取比特币。所以我们认为，这个攻击对51%攻击者来说是不可能的。

我们应该注意到这是一个想象的实验。如果实际中真的有51%攻击的迹象，可能会发生的是开发者会注意到并采取应对措施。他们会升级比特币软件，我们可以期待系统规则（包括点对点网络）可能会做出改变，使得这样的攻击难以成功。但我们无法准确预测。所以，我们是在一个简化的模型上讨论51%攻击，但除此之外系统规则并没有改变和扭曲。

我们考虑另一种攻击。51%攻击者可以压制其他交易吗？比如攻击者特别讨厌某个用户卡罗尔。他知道卡罗尔一些地址，想使属于这些地址的币都无法使用。这可能吗？由于攻击者控制了区块链的共识过程，他可以轻易地拒绝创造包含来自卡罗尔地址的交易的新区块，他还可以进一步拒绝在含有类似交易的区块上延展。但他不能阻止这个交易被广播到整个点对点网络，因为网络不依赖于区块链或者共识，我们假设攻击者还没完全掌控网络。他不能阻止这个交易被发送到绝大部分节点上，所以即使他成功了，大家也都知道发生了攻击。

攻击者可以改变区块奖励吗？比如说攻击者开始假装把区块奖励由25个币改成100个币？这是对系统规则的改动，因为他没有控制所有诚实节点上运行着的比特币软件备份，所以同样不可能。这和为什么攻击者无法装入一笔非法交易的道理是一样的。其他节点不会轻易认可区块奖励提高，所以他也无法使用这些区块。

最后，这个攻击者会摧毁大家对比特币的信心吗？好吧，让我们想象一下会发生什么。如果有很多双重支付尝试，诸如节点不延展最长的有效分支，以及发生其他攻击，那么人们有可能会觉得比特币不再是一

个他们可以信赖的去中心化账簿。人们会对货币失去信心，我们可以预料到比特币汇率会重挫。实际上，如果人们知道有一方控制了51%的哈希算力（hash power），即使这个人没有发动任何攻击，大家也可能会对比特币失去信心。所以，这不仅仅是可能，事实上任何形式的51%攻击都会摧毁大家对货币的信心。这其实是51%攻击可以实现的最主要的实际威胁。考虑到在攻击比特币，实现51%多数的过程中，财政角度的巨大花费，我们讨论的这些攻击都会变得不切实际。

我们希望至此你对比特币的去中心化管理有了一个完整的了解。你也应该理解了比特币里的身份如何工作、交易是如何被传播和验证的、比特币里点对点网络的作用、如何用区块链达成共识、函数难题与挖矿是怎么回事。这些概念为理解比特币的更多微妙细节和细微差别提供了坚实的理论基础，是一个良好的出发点。这些我们在后续章节中会进一步看到。

延伸阅读

比特币白皮书：

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008.

下载地址：<https://bitcoin.org/bitcoin.pdf>.

最初的基于工作量证明的介绍：

Back, Adam. “Hashcash—A Denial of Service Counter-measure.” 2002.

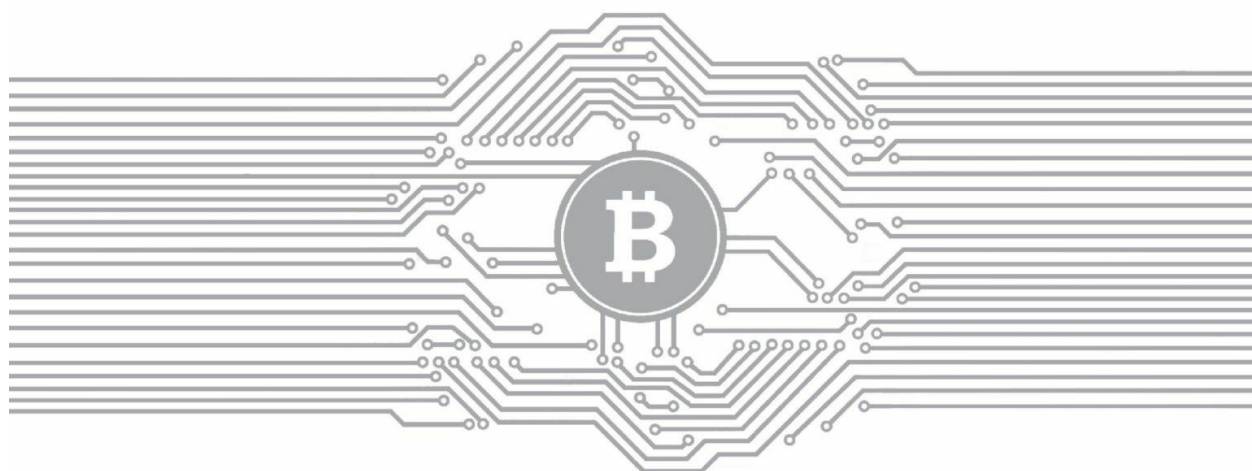
下载地址：<http://www.hashcash.org/papers/hashcash.pdf>.

Paxos共识算法介绍：

Lamport, Leslie. "Paxos Made Simple." ACM Sigact News 32(4), 2001: 18-25.

第3章

比特币的运行机制



在这一章我们重点剖析一下比特币的运行机制。前两章里，我们是在相对泛泛的层面讨论了比特币，在这一章中我们将深入细节，真正近距离地了解比特币所使用的数据结构、实际脚本以及语言，这种较为精准的介绍会为本书后面的章节建立场景。这一章会有大量细节性的信息，极具挑战。本章可以帮助我们真正懂得比特币的实质。

如第2章所述，比特币的共识机制设定了一个只允许往里写入的账簿，而且一旦数据被写入，它将永远被储存在那里。去中心化（或者分布式）协议确保了账簿中存储数据的共识，而矿工会执行协议并确认交易，这些机制可以确保每一笔交易都是真实发生的，而且账簿中的每一个比特币都没有被使用过。这样，这个账簿从功能上就形成了一种货币系统。同时，我们也假设，可以使用货币奖励矿工，使矿工有积极地完成记账操作的动力。在本章中，我们将详细介绍如何建立货币系统、如何奖励矿工，从而保证整个流程有序运行。

3.1 比特币的交易

让我们先一起看一下比特币的交易，比特币交易的过程其实就是不停地创造区块的过程，为了理解上的方便，我们先看一个简单模式的账簿，在这个账簿里，每一笔交易依次被添加到账簿里。

那我们如何使用这个账簿来创造一种货币呢？首先你可能想到（也是许多人误认作比特币使用的方式）：建立一个以账户为核心的系统，可以创造新的币并且放入某人的账号，然后就可以转给其他人了。一笔交易的信息就像这样：“把爱丽丝账户里17个币转给鲍勃”，然后由爱丽丝签名。我们从图3.1可以看到，爱丽丝在第一批交易里收到25个币，然后转了17个币给鲍勃，她的账户里应该还有8个币。

系统制造了 25 个币给爱丽丝，由矿工确认
爱丽丝转了 17 个币给鲍勃，由爱丽丝签名
鲍勃转了 8 个币给卡罗尔，由鲍勃签名
卡罗尔转了 5 个币给爱丽丝，由卡罗尔签名
爱丽丝转了 15 个币给戴维，由爱丽丝签名

图3.1 基于账户的账簿

这么做的不便之处在于，任何人如果想要确认一笔交易是否真实，就必须跟踪每一个账户的余额。让我们再看一下图3.1，当爱丽丝想要转给戴维15个币的时候她是否真的有15个币呢？为了搞清楚这个问题，我们必须回过头去看和爱丽丝有关的所有交易，并加总来确认当时的余额。当然，我们可以有一些更有效的办法，比如另外增加一个数据字

段，用来更新每次交易后的账户余额，但这也增加了记账的工作量。

所以，比特币并没有用这种记账方式，而是用了我们在第1章1.5节里提到的“财奴币”相类似的方法来记录交易。

这种方式就像财奴币里的付币，每个交易中都有一个输入值和输出值。输入值可以看成是将被消费掉的币（这些币是前一个交易创造出来的），把输出看成是在本次交易中创造出来的币。铸造新币时，只会创造新币，而不会消费旧币（就像财奴币里的造币，只有输出，没有输入）。每笔交易都有一个独一无二的ID。每笔交易中可能有多个输出，输出的索引从0开始，所以我们称第一个输出为“输出0”。

我们现在来看图3.2。交易1是铸造新币的交易，因此没有输入，也没有签名；交易1的输出是向爱丽丝转移25个币。现在，爱丽丝想把一些币转给鲍勃，她就创造了一条新的交易，这就是图3.2中的交易2。在交易里，她必须明确指出要转出的币的来源（引用之前的某笔交易）。爱丽丝指出本次交易的币来自交易1中的输出0（也是交易1中的唯一输出），即向爱丽丝转移25个币。交易中，爱丽丝还要明确收款人——也就是输出的地址，在这个例子里，有两个输出，一个是转17个币给鲍勃，另一个是转8个币给爱丽丝自己。当然，整个交易由爱丽丝签名，这样，大家就知道这笔交易爱丽丝是确实授权了的。

1	输入：0 输出：25.0 → 爱丽丝
2	输入：1[0] 输出：17.0 → 鲍勃，8.0 → 爱丽丝 由爱丽丝签名
3	输入：2[0] 输出：8.0 → 卡罗尔，9.0 → 鲍勃 由鲍勃签名
4	输入：2[1] 输出：6.0 → 戴维，2.0 → 爱丽丝 由爱丽丝签名

图3.2 与比特币类似的基于交易的账本

地址转换。 在这个例子里，为什么爱丽丝要把币转给自己呢？事实上比特币就像财奴币中描述的币一样，一个交易中输出的币，要么在另一个交易中被完全消费掉，要么就一个都不被消费，不存在只消费部分的情况。爱丽丝只需付给鲍勃17个币，但爱丽丝在上一交易中实际获得了25个币，为了把这些币全部消费掉，她必须再转给自己8个币。这8个币可以转到另外一个地址（不同于交易1中获得25个币的地址），但前提是该地址为爱丽丝所有，这就叫地址转换。

有效验证。 当一个新的交易被加入总账，它的有效性是否容易被验证？在这个例子里，我们要核查一下爱丽丝引用的交易输出，确认她确实有25个币没有被花费掉。因为我们使用了哈希指针，所以核查很快。为了确认这25个币没有被花掉，我们只需从爱丽丝所引用的交易开始，一直核查到账本上最新记录的交易为止即可——而不需要从账本建立之初的交易开始核查。而且，这种方法也不需要增加额外的数据结构（当然，我们将会看到，加入新的数据结构将进一步提高速度）。

资金合并。 和财奴币一样，比特币交易可能有许多输入与输出，资金分隔与合并也很容易。假如鲍勃在两笔不同的交易中分别收到17个币和2个币，现在他想把这两笔钱合并起来花掉，这很容易，他只需发起一个交易，交易里有两个输入和一个输出，输出的地址是他自己的地址，这样，鲍勃就把两个交易合二为一了。

共同支付。 同样地，共同支付也很容易做到。如果卡罗尔和鲍勃想要共同支付给戴维，他们可以发起一个交易，交易里也有两个输入和一个输出，唯一不同在于，两个输入所引用的“上一笔交易”的输出地址不同，因此，这笔交易需要两个签名：卡罗尔的和鲍勃的。

交易语法。 比特币交易涉及的概念就是上面这些。我们再来看看比特币交易在底层是如何实现的。实际上，比特币在网络上传输的数据结构都是一串字符，图3.3显示了一个真实的程序，经过编译就会变

成供机器执行的二进制代码了。



图3.3 一个真实的比特币交易程序段

从图3.3可以看到，一个比特币交易分成三部分：元数据、一系列的输入和一系列的输出。

● 元数据。这里存放一些内部处理的信息：包含这笔交易的规模、输入的数量、输出的数量，还有此笔交易的哈希值，也就是这个交易独一无二的ID。我们可以用哈希指针指向这个ID。最后还有一个“锁定时间”（lock_time），我们后面会谈到。

● 输入。所有输入排成一个序列，每个输入的格式都是一样的。输入需要明确说明之前一笔交易的某个输出，因此它包括之前那笔交易的哈希值，使其成为指向那个特定交易的哈希指针。这个

输入部分同时包括之前交易输出的索引和一个签名：我们必须有签名来证明我们有资格去支配这笔比特币。

● 输出。所有输出也排成一个序列。每个输出的内容分成两部分。所有输出的金额之和必须小于或等于输入的金额之和。当输出的总金额小于输入总金额时，输出的总金额与输入的总金额的差额部分，就作为交易费支付给为这笔交易记账的矿工。

一长串怪怪的（funny）字符看上去像是接收地址。实际上，每个输出都要和一个特定的公钥（地址）对应，所以这一长串字符里面确实有一部分看上去是公钥的哈希值，但里面还有一部分看上去像指令集合的东西，它其实是一个比特币的脚本，下文展开介绍。

3.2 比特币的脚本

每个交易输出不仅确定了一个公钥，其实同时指定了一个脚本。那脚本是什么？为什么我们要用一个脚本？在这一节我们要学习比特币的工作控制语言，也叫脚本。之后，我们就会懂得为什么要用一个脚本，而不是简单地分配一个公钥。

最常见的比特币交易，就是通过某人的签名去取得他在前一笔交易中获得的资金。这种情况下，我们希望交易的输出包含这样的信息：“凭借地址X的所有者的签名，才可以获得这笔资金。”我们知道地址其实就是一个公钥的哈希值，所以仅仅说地址X并没有告诉我们公钥在哪里，也没有给我们一个检查签名的方法。所以，交易输出必须这样描述：“凭借哈希值为X的公钥，以及这个公钥所有者的签名，才可以获得这笔资金。”这实际上就是最常见的比特币脚本，如图3.4所示。

```
OP_DUP
OP_HASH160
69e02e18...
OP_EQUALVERIFY
OP_CHECKSIG
```

图3.4 P2PH脚本范例

注：一个常见的比特币输出脚本范例。

那么谁执行这个脚本？这一系列指令是如何完成的呢？秘密在于，交易的输入包括了脚本（而不是签名）。为了确认一笔交易正确地获取了上一笔交易所输出的资金，我们把交易的输入脚本和上一笔交易的输出脚本串联起来，这个串联脚本必须被成功地执行后才可以获取资金。

这两个脚本，一个是输出脚本（scriptPubKey），另一个是输入脚本（scriptSig）。输出脚本只是指定了一个公钥（或是公钥哈希值的地址），输入脚本指定了一个对应公钥的签名。图3.5就是两个脚本结合的案例。

比特币脚本语言

这个脚本语言是为比特币开发的。在比特币里只叫作“脚本”。它和另一种Forth语言有很多相似的地方，Forth是一种简单的堆栈式编程语言（stack-based programming language），但你并不需要先学习Forth语言才会使用比特币的脚本语言。比特币的脚本语言设计原则就是简明扼要，并内生地支持加密操作。比如，脚本里面有目的性的指令用来计算哈希值和检验签名。

这种脚本语言是堆栈式的，意味着每个指令只被执行一次，是线性的，无法循环执行。所以指令的数目给了我们一个执行时间与内存使用的上限。这个语言不是图灵完备的，意味着不能随意运行强大函数功能。[\[1\]](#)但这是有意设计的，因为矿工需要去执行这些网络上任意交易提交者所递交的脚本，设计者并不希望让他们提交可能无限循环的脚本。

```
<sig>
<pubKey>
-----
OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG
```


图3.5 结合输入脚本和输出脚本范例

注：为了确认当前交易是否正确地获取了前一笔交易输出的资金，我们把两个脚本链接起来，把上一笔交易的输出脚本（图中虚线下方）添加到当前交易的输入脚本（虚线上方）之后，形成一个新的脚本。请注意<pubKeyHash?>里面有一个“？”，用作标识——我们后面会来确认它是否与当前交易提供的公钥的哈希值一致。

执行比特币脚本只能产生两个结果：要么被成功执行，这种情况下，交易有效；要么脚本执行出现错误，这种情况下，整个交易无效，拒绝记入区块链。

这个脚本语言十分简单。只有256个指令，每个只用一个字节。256个指令中，有15个目前不可用，有75个被保留还没有具体定义（以后或许可以被用来扩展），剩下的才是可用的。

许多在其他语言里常见的基本指令这里面都有。例如，基本的算数、逻辑语句（如If-then）、抛出错误、过早返回等。而且，还有密码指令，比如哈希函数语句、签名验证语句，还有一个重要的特殊指令是“CHECKMULTISIG”——可以查证多个签名。表3.1列举了一些比特币工作控制语言里的常用语句。

CHECKMULTISIG指令要求指定n个公钥和一个参数t（作为一个临界值）。这个指令正确执行的条件是：在n个公钥中，至少可以选出t个现时有效的签名。我们在本章3.3节会示范这个指令的用法，但现在我们需要认识到这个原生指令是非常强大的，它以一种极其精练的方式协助我们查验交易中的多方签名。

不过，目前比特币多方签名功能实现过程中有一个缺陷，CHECKMULTISIG指令在执行的时候会返回一个没用的值，而且系统还必须要安排一个堆栈中的变量去储存它，然后再忽略掉。由于修复这个缺陷成本很高，两害相权取其轻，这个缺陷就一直没被修复，我们在第3章3.6节会再做讨论。但目前，这个程序缺陷也算是比特币的一个特性。

表3.1 一些比特币脚本工作语言中的指令及其功能

指令名称	功能
OP_DUP	复制堆栈顶端数据
OP_HASH160	计算哈希函数两次：第一次用 SHA - 256，第二次用 RIPEMD - 160
OP_EQUALVERIFY	如果输入是相同的，返回真 如果输入是不同的，返回假，整个交易作废
OP_CHECKSIG	检查输入的签名是否有效
OP_CHECKMULTISIG	检查在交易中 t 个公钥（地址）对应的 t 个签名是否有效

执行一个脚本

在堆栈语言里执行一个脚本，我们只需要一个堆栈来垒积数据，不需要分配任何内存与变量。因此，堆栈语言中计算相当容易。总共有两类指令：数据指令和工作码指令。数据指令的作用是把数据推到堆栈的最上面；工作码指令则通常是用堆栈顶部的数据作为输入值，用来计算一个函数。

我们现在来一起看一下，图3.5这段脚本是怎么执行的。图3.6给我们展示了每一条指令执行后的堆栈状态。脚本中的前两条指令属于数据指令，分别是输入脚本（包含在交易的输入项）中的签名和用来验证签名的公钥。我们前面提到过，一看到数据指令，系统就把它堆到堆栈最上面。后面几个指令是输出脚本（包含在上一交易的输出项中）里的指令。

首先，我们复制指令OP_DUP，这一步仅仅是将堆栈最上层的公钥复制，并置于堆栈最上层；下一个指令是OP_HASH160，该指令取得堆

栈最上层的数据，并计算其哈希值，然后将结果再堆到堆栈最上层。当指令执行完成后，我们将堆栈最上层的公钥替换成了公钥的哈希值。

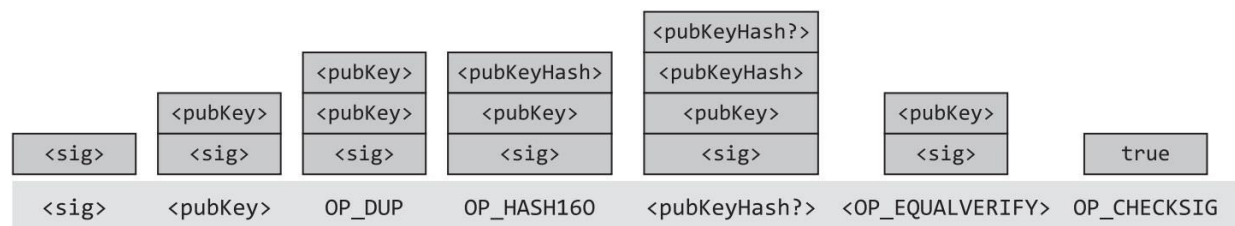


图3.6 比特币脚本的执行堆栈状态图

注：图中底部列出了相对应的指令：尖括号里的是数据指令，以OP开头的是工作码指令，指令上方对应的是指令执行之后的堆栈状态。

接下来，我们还要在堆栈顶层再推送一些数据：此笔交易发送者指定的公钥的哈希值，以及对应的私钥，这样才可完成签名，取得资金。此时，堆栈顶部有两个数值，一个是发送者指定的公钥的哈希值，另一个是接收者想要取得资金时提交的公钥的哈希值。

这个时候，我们就要执行EQUALVERIFY命令了，这个命令是用来检查堆栈顶部两个数值是否相等的。如果不相等，就会抛出一个失败信号，并且停止执行脚本。不过现在我们假设其相等，也就代表着接收者使用的是正确的公钥。这条指令会移除堆栈顶部的两条数据，这时，堆栈还剩下两个数据：公钥以及签名。

我们已经证实接收者使用的公钥确实就是交易里指定的公钥，但现在我们必须证实这个签名是真的。这时，使用OP_CHECKSIG指令即可。这里我们可以看出比特币的脚本语言虽然简单，但很强大。它只用“OP_CHECKSIG”就能实现一个很复杂的事情：移除堆栈里两个数值，然后用公钥来证实整个交易的签名是真的。

但这里的签名究竟是对什么的签名？签名函数的输入是什么？实际上，在比特币中，我们只可以对一个事情进行签名——就是整个交易。所以，CHECKSIG指令从堆栈中取出两个数据（公钥以及签名），并验

证签名对于整个交易（使用对应公钥发起的交易）来说是有效的。现在我们完成了所有的指令，堆栈里面什么也不剩。假设没有碰到任何差错的话，这个脚本的输出就是一个“真”表示这个交易是正当有效的。

实际情况

理论上讲，通过脚本，我们可以随意地为比特币支付设定条件。当然，从2015年的情况看，这些特性也并不太常用到。如果我们回顾比特币历史中曾经实际用到的脚本，绝大多数的比特币使用的脚本都非常基础，像前文的例子一样：指定一个公钥，然后通过验证签名来使用这个币。

当然，实际中也会使用一些其他指令，比如MULTISIG，还有一种支付给脚本的哈希值（Pay-to-script-hash，简称P2SH，我们很快会谈到）等，但除此之外，平时常用的指令真不多，因为每个节点都有一份标准脚本的白名单，它们会拒绝接受不在名单上的脚本。这倒不是说无法运行其他脚本，只是使用起来比较麻烦。事实上这样的安排也很巧妙，我们会在谈论比特币点对点网络的时候再进行描述。

销毁证明

销毁证明（proof of burn）脚本，用于销毁比特币（即防止资金被赎回）。如果交易代码的运行结果是将比特币转到“销毁证明”脚本，那么这笔比特币将被销毁。实际应用中主要是用来引导客户使用其他数字货币系统，即将比特币销毁，以便获得另一个数字货币系统发行的新币。我们会在第10章展开叙述。销毁证明脚本使用起来非常简便：使用OP_RETURN脚本来抛出错误；不论之前指令的运行结果是什么，OP_RETURN指令总会被执行，并相应抛出一个错误，脚本返回一

个“错误”(false)值。

由于OP_RETURN以抛出错误的形式结束脚本，其后的所有指令都不会执行。利用这个特性，我们可以往脚本中植入任意信息，这些信息也将被存储在区块链中。假如你想通过署名或者盖时间戳的方式来证明你在某个时候知道某件事情，就可以发起一笔极小额的比特币交易，在脚本中加入上述信息，并使用销毁证明脚本将币销毁，这样就可以将信息永久地存储在区块链上。

支付给脚本的哈希值

如前文所述，比特币的工作机制要求币的发送者必须在交易时明确指定脚本。这种机制有时候不太适用：假如你在网店看中了一件商品并打算下单，你会问卖家“请把付款地址告诉我，我可以付款了”，但如果卖家使用了多重签名地址（MULTISIG），那他会说“嘿，我们用了多重签名地址，你需要支付给一个脚本地址，而不是一个简单的地址”，但你会说“我不知道怎么弄，这太复杂了，我只会支付给简单的地址”。

比特币用了一种很聪明的办法来解决这个问题，不仅可以实现多重签名地址支付，而且还可以实现复杂的资金监管规则。比特币使用的办法是：收款方告诉付款方“请把比特币支付给某个脚本地址，脚本的哈希值是xx，在取款的时候，我会提供上述哈希值对应的脚本，同时，提供数据通过脚本的验证”，而不是“请把比特币支付给某个公钥，公钥的哈希值是xx”。付款方通过P2SH即可实现上述交易。

需要说明的是，P2SH脚本只是对堆栈最顶层的数据进行哈希运算，核验运算结果是否与给定的哈希值一致，核验通过后，再执行一步特殊的核验：将堆栈最顶层的数据重新解读为一系列指令，然后将其作为脚本运行一次，此时，堆栈中的其他数据作为脚本的输入值。

要做到P2SH还是有点复杂的，因为P2SH不是比特币的原始设计，是后来加上去的。它解决了两个重要的问题：让付款方的支付工作简单化，收款方只需告诉付款方一个哈希值即可。在我们上面的例子中，你不再需要去关心商家到底用哪种地址，是否用了多重签名，因为这只是商家在支取这笔款项时需要考虑的事情。

P2SH还实现了效率上的提升：矿工的工作是追踪那些还没有被消费掉的输出脚本。采用P2SH的输出脚本会变得很小——它们只不过是哈希值而已。所有的复杂性都被放在输入脚本中了。

[1] 图灵是第二次世界大战时英国数学家，密码学家。他破译了纳粹的密码机“谜”，为盟军取得第二次世界大战胜利做出重大贡献，美国好莱坞以此题材拍了一部电影《模仿游戏》。图灵完备的意思是语言有能力随意地执行强大的函数。——译者注

3.3 比特币脚本的应用

现在我们已经明白了比特币脚本的工作机制，接下来我们看一下比特币脚本语言的一些强大应用。你立刻就能明白，比特币将指定公钥变成复杂地指定脚本，是有实际意义的。

第三方支付交易

比如，爱丽丝用比特币向鲍勃买东西，爱丽丝想货到付款，而鲍勃想见款发货。该如何处理？一个好的办法是使用**第三方支付交易**（escrow transaction）。

第三方支付交易可以用“MULTISIG”（多重签名）来轻易实现。爱丽丝并不直接付款给鲍勃，而是发起一个多重签名的交易，并规定：三个人中有两人签名之后，资金才能被支取。这三个人是爱丽丝、鲍勃与第三方仲裁员朱迪（Judy）。朱迪负责调解可能发生的纠纷。因此，爱丽丝发起了一个2/3的多重签名交易来付款，这个交易规定三个人中有两人签名之后，资金才能被支取。这个交易被纳入区块链后，资金被第三方监管，这三个人中的任意两个人可以决定资金的去向。现在，鲍勃觉得可以给爱丽丝发货了，通常情况下，如果爱丽丝和鲍勃都是有诚信的，鲍勃会按照爱丽丝要求发货，爱丽丝收货之后和鲍勃共同签名，把资金转给鲍勃。由于三个人中有两人签名即可完成支付，此时，由于没有任何争议，朱迪根本不需要参与。和爱丽丝直接付款给鲍勃相比，第三方支付交易并不会更复杂，只需在区块链里增加一笔交易即可。

但如果鲍勃其实并未发货，或者货物在路上被弄丢了，又或者鲍勃发的货物并不是爱丽丝想要的，这时会出现什么情况？爱丽丝觉得被骗

了，所以不打算付款给鲍勃，而是想把比特币从监管账户要回来。这种情况下，爱丽丝不会签名真正完成付款，而鲍勃肯定也不会承认问题而主动放弃收款，这时，就需要朱迪判定资金到底该转给谁。如果朱迪认为鲍勃欺骗爱丽丝，她就会跟爱丽丝一起签名，把比特币退还给爱丽丝，当然，如果她认为爱丽丝应该付款，那她就会和鲍勃一起签名，完成资金的实际支付；所以，到底该完成支付或是撤销支付，由朱迪决定。当然，这种情况也只有在发生纠纷时才出现。

绿色地址

另外一个很酷的应用叫作**绿色地址**（green addresses）。假如爱丽丝要转账给鲍勃，而鲍勃不在线（或者鲍勃在线但没有时间），所以他无法通过查看区块链的更新来确认转账是否完成。一般来说，一个交易需要获得6次确认，我们才能确信它已经确实被加到区块链中，但这需要大约一个小时。但是，想象一下，如果爱丽丝只是在鲍勃的店里买一个热狗，这么长时间才确认交易，显然是不可接受的；或者，如果鲍勃由于某些原因无法接入互联网，那他就一直无法确认交易。

为了解决这个问题，比特币采用了第三方银行的做法，实际上，“银行”可能是一个交易所，或者是其他的金融媒介。如果爱丽丝要转账给鲍勃，爱丽丝会和她的银行联系，“我要付给鲍勃这些币，你能办理吗？”银行会回答：“好的。我会从你的账号扣钱，然后从我的绿色地址转账给鲍勃。”这样，收款人就不需要实时查看区块链来确认交易。

需要注意的是，款项并不是由银行直接支付给鲍勃，实际上，部分款项，可能会通过其他地址回到银行手中。但是，由于比特币从银行控制的某个账户——我们在此所称的“绿色账户”直接转给鲍勃，而且，银行保证它不会双重支持这个比特币，如果鲍勃也相信这一点，当他看到

银行签名的交易时，就可以确认自己迟早会收到这些比特币——只要区块链确认这笔交易。

请注意，这不是比特币技术系统的保证，而是现实世界中银行的保证，银行为了保护它的声誉，不会双重支持比特币。银行可以向客户证明，“我一直使用这个账户来支付，从始至终也没有发生过双重支付，我以前没有这么做，以后也不会这么做。”如果鲍勃信任银行不会进行双重支付的承诺，他就无须信任爱丽丝——他对爱丽丝本来就了解不多。

当然，如果银行出现了双重支付事件，它就会自毁长城，人们不会再信任它。实际上，有两个提供绿色地址的机构 [Instawallet和门头沟公司 (Mt.Gox的昵称，位于日本东京，是全球最大的比特币交易商)] 就是由于失信而倒闭的。目前，绿色地址使用得越来越少：最初，人们认为绿色地址可以实现快速支付，而且不需要通过查看区块链来确认交易结果；但是现在，人们认为，对“银行”过分信任是有风险的。

高效小额支付（efficient micro-payments）

我们再举一个比特币脚本应用的例子。假设爱丽丝是鲍勃的客户，需要持续向鲍勃支付小额费用，例如，鲍勃是爱丽丝的手机流量提供商，根据爱丽丝每分钟使用的流量计费。但是，每分钟支付一次是不现实的：即使技术上做得到，交易手续费也让人吃不消。

我们希望能把每分钟的费用累积起来，最后一次性支付。为了实现这种想法，爱丽丝先发起一个MULTISIG交易，把可能花费的最大金额转到MULTISIG地址，但这个交易需要爱丽丝与鲍勃两个人的签名才能生效。爱丽丝在使用流量的时候，每隔一分钟就签名一次，向鲍勃支付这分钟所产生的流量费用，然后把剩余的钱转给自己，每分钟重复一

次，直到挂机为止。请注意，这些交易只有爱丽丝的签名，还没有鲍勃的签名，因此，交易还没被放进区块链里。爱丽丝挂机之后，会告诉鲍勃“我用好了，你可以切断我的服务了”，此时，爱丽丝将不再支付费用，鲍勃也将切断服务，然后在爱丽丝发送的最后一个交易里签名，把它放入区块链里。

随着每个交易付给鲍勃的币越来越多，爱丽丝的币就会越来越少。最后一个交易会一次性向鲍勃支付所有的流量费，然后把剩余的币还给爱丽丝。整个过程中，爱丽丝单独签名的交易不会进入区块链（上面没有鲍勃的签名），最后它们都会被丢弃掉。

从技术上讲，所有这些交易都是双重支付。在介绍绿色地址时，我们特别提到防止双重支付的重要性，但在本例中，我们却主动创造了大量的双重支付。实际上，如果双方都是正常运作的话，鲍勃只会在最后一个交易上签名，所以我们在区块链上看不到中间产生的那些双重支付交易。

还有一个微妙的细节：如果鲍勃没有在最后一个交易上签名呢？他可能会说，“就让那些币待在第三方托管地址里吧。”这样一来，爱丽丝就会失去她一开始转到MULTISIG地址的所有比特币。但我们有一个聪明的办法来解决这个问题，那就是我们前面看到的一个代码——锁定时间。

锁定时间

为了避免上面说的这个问题，在小额支付协议开始之前，爱丽丝与鲍勃要签订一个交易，约定向爱丽丝退还所有的比特币，但是这个“退款”行为被上了锁，直到锁定时间到了为止。爱丽丝发起MULTISIG交易把比特币转入第三方托管之后，在向网络宣布这笔交易之前，她会从

鲍勃那里要求这个退款交易。这样，如果过了t时间鲍勃还没有在最后一个交易上签名的话，她可以通过这个退款交易收回所有的比特币。

退款交易被锁定t时间是什么意思呢？还记得我们在第3章3.2节提到元数据的时候，有一个参数是“lock_time”，当时我们还没有解释。在此参数后面填上非零数值t，这个值告诉矿工在记账的时候，要等待t时间之后才能把这笔交易记入区块链。这个交易在放入区块后，经过确定的区块数或者时间才生效。通过这种方式，人们可以发起一笔未来交易，当然，只有资金在未来时间点之前未被花费掉，这笔未来交易才会被执行。这在小额支付的例子里非常有效，它是爱丽丝的定心丸，能够确保在鲍勃最后没有签字的情况下她能拿回自己的比特币。

通过上面的例子，我们展示了比特币脚本可以轻易实现很多功能。我们虽然只讨论了三个例子，但其实人们研究过许多其他的功能。比如多人彩票系统，这个系统涉及一些十分复杂的多步操作协议，以及不同的锁定时间和第三方托管账户，来防止玩家作弊。还可以通过脚本语言实现多人混币，使得比特币更难被追踪。我们会在第6章展开讨论。

智能合约

所谓**智能合约**（smart contracts），就是那些不同于需要通过法律或者仲裁机构来保护执行的普通合约，智能合约是比特币系统里可以用技术手段来强制执行的合约，我们已经看到，比特币有非常好的特性让我们可以用脚本、矿工和交易验证——而不是通过中心化权威机构——来实现第三方托管协议或是小额支付。

智能合约的研究目前已经非常深入，能够实现非常多很复杂的功能，但比特币脚本语言的设计也有很多缺陷，还是有很多现实需要的智能合约无法用比特币的工作控制语言来实现^[1]。不过这里我们就不一一

细谈了。

[\[1\]](#) 但已经有很多有意义的探索，比如以太坊等实现了图灵完备的智能合约。——译者注

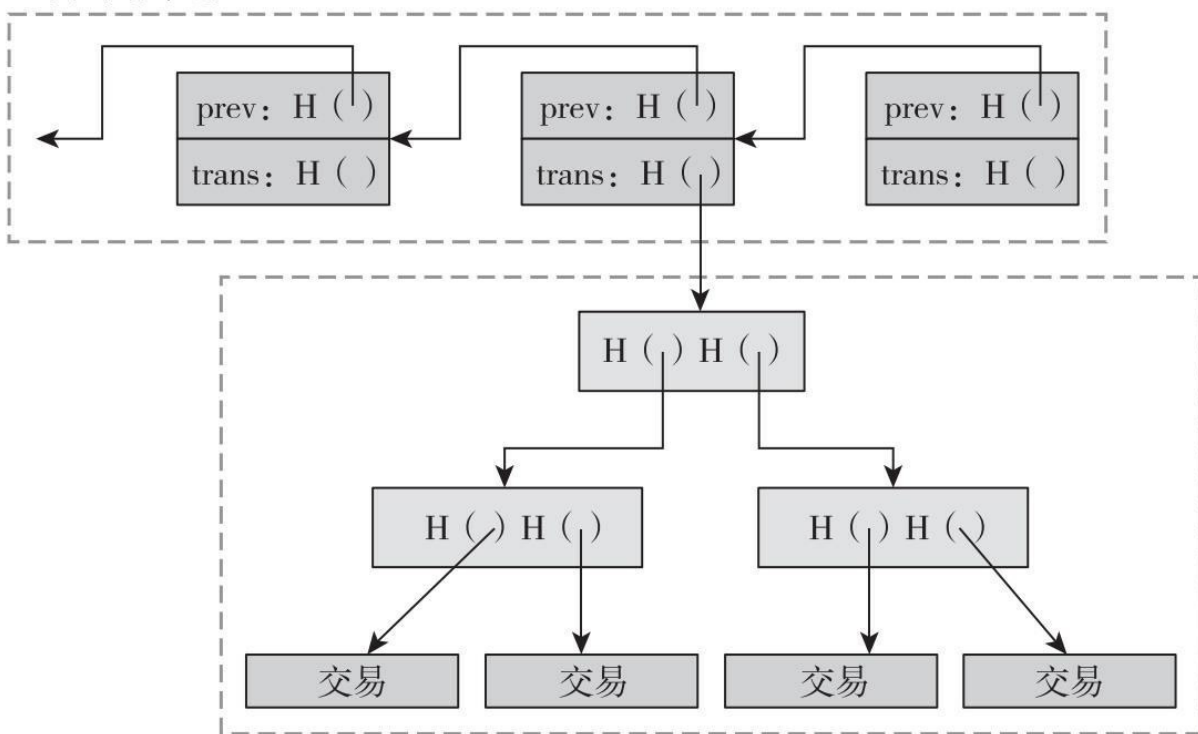
3.4 比特币的区块

现在，我们已经了解了单个交易是如何创建的，但是在第2章里提到，所有交易都是被打包放入区块的，为什么要这么做呢？其实这是为了性能优化，如果每一个交易都要矿工单独去达成共识，那整个系统的交易处理速度将会变得非常慢。而如果我们把大量交易组织起来放入一个区块，得到的哈希链就更短，大大提高了验证区块链数据结构的效率。

区块链（块链）非常聪明地把两个基于哈希值的数据结构结合起来：第一个数据结构是区块的哈希链，每一个区块都有一个区块头部，里面有一个哈希指针指向上一个区块。第二个数据结构是一个树状数据结构，也就是以树状结构把区块内所有交易的哈希值进行排列存储。也叫梅克尔树（请参考第1章），它以一种非常高效的形式把所有交易组织起来。为了证明某个交易在某个区块内，可以通过树内路径来进行搜索，而树的长度就是区块内所包含的交易数目的对数（见图3.7）。

我们在第2章中提到过（在第5章还将继续涉及），区块头部还包含了挖矿谜题^[1]相关的信息。还记得，区块头部的哈希函数必须以一大堆零开头才有效，此外，区块头部还要包含一个矿工可以修改的“临时随机数”、一个时间戳和一个点数（点数用来表示找到这个区块的难度）。区块头部是挖矿过程中唯一哈希值化的，所以要验证一个区块的链，只要检查区块头部即可。在区块头部唯一的交易数据是交易树的树根——“mrkl_root”。

区块的哈希链



每个区块中各笔交易的哈希树（梅克尔树）

图3.7 比特币的区块链有两个哈希结构

注：一个就是把区块联结在一起的哈希链，另一个就是区块内部的交易哈希值梅克尔树。

每个区块的梅克尔树上都有一个有意思的交易，叫作币基交易（见图3.8）。这就类似于财奴币里的造币交易。这个交易创造新的比特币，它看上去像是一个普通的交易，但有几点不同：


```

    "in":[
      {
        "prev_out":{
          "hash":"000000.....0000000",
          "n":4294967295
        },
        "coinbase":"..."
      },
      [
        "out":[
          {
            "value":"25.03371419",
            "scriptPubKey":"OPDUP OPHASH160 ..."
          }
        ]
      ]
    ]

```

图3.8 币基交易

注：币基交易创造新的比特币，这个交易并不消费之前交易输出的比特币，因此，没有指针指向“上一交易”。币基交易的参数可以是任意数据。币基交易的价值等于区块奖励加上区块中包含的所有交易费。

- 1.它永远只有一个单一的输入与单一的输出。
- 2.这个交易并不消费之前交易输出的比特币，因此，没有指针指向“上一交易”。
- 3.这个输出值目前大约是25个币多一点点。这个输出值就是矿工的挖矿收入。它由两部分组成：一部分是奖励的25个比特币（奖励在每生产210 000个区块——大概4年——后减半），另一部分是所有交易的交易手续费。
- 4.还有一个特别的地方就是“币基”参数，矿工可以放任何值进去。

这里值得一提的是，当比特币的第一个区块被铸造出来的时候，该区块的币基参数提及了伦敦《泰晤士时报》的一则报道：2009年1月3日，财政大臣拯救银行。这被看成比特币发明的政治动机，同时也很好地证明了第一个区块的打包时间是在2009年1月3日，上述报道出来之后。这也是矿工使用“币基”参数来支持很多比特币的不同特性。

想更好了解比特币的区块和交易结构，最好的办法是自己浏览区块链的数据，有很多网站提供数据，比如blockchain.info，在该网站上可以看到所有交易，以及每笔交易所引用的上一笔交易。由于比特币的数据都是公开的，一些程序员已经开发出了全图形化的展现方式。

[\[1\]](#) 也就是竞争记账权利问题。——译者注

3.5 比特币网络

到这里，我们已经讨论了参与者可以发布交易，并将交易纳入区块链，这一切似乎很神奇。事实上，上述整个过程都是通过比特币网络完成的。比特币网络是一个点对点的网络，沿用了很多已有的点对点网络的理念。在比特币网络里，所有的节点都是平等的。没有等级，也没有特殊的节点，或所谓的主节点。它运行在TCP网络上，有一个随意的拓扑结构，每个节点和其他的随机节点相连。新的节点也可以随时加入。可以试着现在就下载比特币节点软件，把你的个人电脑注册为一个节点，这个节点的权限和比特币网络里所有其他节点都是一样的。

由于随时有新的节点进入，也有旧的节点离开，所以比特币网络事实上一直在变化。并没有强制的规定节点何时明确地离开网络，只要一个节点有3个小时没有音讯，就会慢慢地被其他节点忘记。通过这种方式，网络非常缓和地处理节点下线问题。

上文提到，每个节点和其他随机节点相连，网络中并不存在一个确定的地理学意义上的拓扑结构。那么一个节点是如何加入网络的呢？当你启动一个新节点的时候，先向一个你知道的节点发送一个简单的消息。这个节点就是你的种子节点，当然，有多种不同的方法可以查找种子节点。然后你就会问你的种子节点是不是还知道其他什么节点？在链接到一个新的节点后，你可以重复这个过程许多次，最后你可以选择和哪些节点相连，这时，你就成为比特币网络里一个完全合格的节点了。这些步骤里有很多随机性，理想的情况就是你能和一些随机组的节点相连。为了加入网络成为网络节点，你只需知道一开始怎么和其中一个节点链接就行了。

那加入网络到底有什么好处？当然是为了维护区块链。当我们发起

一个交易的时候，我们想让整个网络都知道。这是通过一个“泛洪”（flooding）的算法完成的[有时候我们称之为“八卦”（gossip）协议]。如果爱丽丝要转账给鲍勃，她的客户端发起一个交易，然后把这笔交易告知所有和她的客户端节点相链接的其他节点，这些节点会进行一系列核验，决定是否接受并转播这笔交易。如果核验通过，这些节点会将这笔交易信息传播给与其相连的其他节点。当节点接收到一个交易信息后，会把交易放入一个交易池，但需要注意的是，交易池里的交易还没有被打包进区块链。如果节点接收到的交易在交易池里已经存在，就不会再次把它传播出去。这样，就确保了泛洪协议会自动终结，而不是让一个交易在网络一再被传播永不停止。由于每个交易都有一个独一无二的哈希值，所以节点可以非常方便地查询某个交易是否在自己的交易池里。

节点接收到一个新交易信息时，如何核验呢？这里有四个关卡：第一个也是最重要的一个是交易验证，也就是验证交易在当前的区块链中是有效的，节点会针对每个前序交易的输出运行核验脚本，确保脚本的返回值都为真；第二，检查是否有双重支付；第三，如前文所述，节点会检查这笔交易信息是不是已经被本节点接收过；第四，节点只会接收和传递在白名单上的标准脚本。

上述所有检查都是合理检查，所有节点很好地执行这些检查能够使网络健康、稳定地运行，但实际上并没有规则强制节点执行这些检查。虽然如此，每个节点还是有必要进行检查的——因为比特币网络是一个点对点的对等网络，任何人都可以随时加入，总有一些节点会发出双重支付，或者非标准脚本的交易，甚至彻底就是非法交易。

由于网络传递有延迟，不同的节点可能会有不同的交易池。当有双重支付攻击的时候，这个现象会变得十分有意思。假设爱丽丝想把同一个比特币支付给鲍勃与查理，于是，爱丽丝几乎同时发出两笔交易。有些节点先听到爱丽丝→鲍勃交易，有些则先听到爱丽丝→查理交易。当

一个节点接收到了这两个交易当中任何一个，它就会把接收到的交易放入交易池中，之后，它听到了另一个交易，看上去像是双重支付交易，这个节点就会把它丢弃掉不再向外传播。结果就是众多的节点会对“哪一个交易应该被纳入区块链”产生分歧。这种情况被称为竞态条件^[1]（race condition）。

好在对于比特币来说，这完全不是问题：打包下一个区块的矿工会打破这个僵局，他会决定哪个交易会最终打包进这个区块。如果爱丽丝→鲍勃的交易进入区块，那些听到爱丽丝→查理节点会把爱丽丝→查理的交易从交易池里剔除，因为那是一个双重支付；而那些听到爱丽丝→鲍勃的节点也会把这个交易剔除出去，因为这笔交易已经被纳入区块链。因此，一旦这个区块被传播以后，就不再有前面说的分歧了。

由于每个节点默认保留最早接收到的交易，所以节点在网络上的位置就很重要。如果两个矛盾的交易或区块在网络上两个不同地方被发起，它们会同时向整个网络广播，节点先接收到哪个交易取决于它在网络的位置。

当然，这基于一个假设：不管接收到什么信息，每个节点均保留最早接收到的交易。但是比特币网络是一个对等的网络，节点并不被强制要求这么做，任何节点都有权按照其他逻辑行事，并按照所选的逻辑决定到底保留哪个交易、转播哪些交易，我们会在第5章的矿工奖励部分讨论这个问题。



零验证交易和费用替代策略(replace-by-fee)

在第2章我们讨论了零验证交易，即一旦交易在网络中广播，接

收方就立即接受交易。零验证交易不是用来防止重复支付的，但由于矿工的缺省行为是把先接收到的交易放入交易池，这样，在零验证交易里就很难实现重复支付，同时，由于零验证交易非常方便，因此变得越来越普及。

自从2013年，矿工的缺省行为变成了“费用替代策略”，即节点在遇到有冲突的交易时，会把交易手续费更高的交易放进自己的交易池，把手续费更低的替换出去。站在矿工的角度，由于收益更高，因此也是理性的选择——至少在短期看是这样。但是这种费用替代策略却使多重支付攻击变得更容易了。

因此，费用替代策略受到了不少争议，这些争议一方面从技术层面讨论在费用替代策略中是否可以真正阻止多重支付；另一方面从哲学层面讨论比特币是不是应该要尽可能支持零验证，或直接放弃费用替代策略。我们这里就不再赘述这些讨论了很久的争议了，但最近比特币核心代码倒选用了“有选择权的”（opt-in）费用替代策略的做法，也就是交易可以标记自己是否适用费用替代策略。

上面说的是交易的传播。至于区块的传播，即矿工挖到一个矿（打包一个区块），然后将区块加入区块链，这个过程与新交易的传播过程类似，也受同样竞态条件的限制。如果两个有效的区块同时被挖到（也就是有两个矿工同时获得了记账权力时），只有其中一个区块可以进入长期共识链，哪个区块被最终纳入长期共识链取决于其他节点选择在哪个区块上扩展区块链，未被纳入的一个即被丢弃。

核验一个区块要比核验一个交易复杂得多。除了确认区块头部，确定里面的哈希值是在可以接受的范围内，节点还必须确认区块里的每个交易。最后，一个节点往外传播的区块必须是最长的一条区块链上新加入的区块（当然，“最长的区块链”取决于节点对区块链当前状态的认识）。只有这样才可以防止区块链分叉。但就像传播交易时一样，节点

同样可以执行它自己的逻辑：它可以选择传递无效的区块，也可以选择传递在共识链上更早加入的区块而不是最新加入的区块。这样就会造成一个分叉，不过这种情况是协议可以承受的。

泛洪算法（flooding algorithm）的延迟情况到底怎样呢？我们一起看一下图3.9，这张图展示了区块被网络中不同数量的节点接收所花费的时间（秒）。三条线分别代表区块被网络中25%、50%、75%的节点接收到所需要的时间。可以看到，由于网络带宽的限制，比较大的区块需要30秒左右才能传播到大部分的节点。所以这个协议不是很有效率。在互联网上30秒是比较长的时间了，在比特币的设计里，简便是第一位的（简单的网络、节点可随时加入或退出），而效率是第二位的，所以在比特币网络里，一个区块可能需要经过很多节点才到达最远的节点。如果网络采取自上而下的设计，那我们就需要使任何两个节点的距离都很短。

网络大小

比特币网络大小很难测量，因为它随时都在变化，而且没有一个中央权威机构。有些人通过研究给了一些估计：往高说，每个月可能有100万个IP地址成为比特币网络的节点（也可能是临时成为节点）。往低说，大约只有5 000~10 000节点永远在线并处理交易。这个数字有点出乎意料得小，但是截至本书完成时，并没有证据表明永远在线的节点数量在升高或降低。

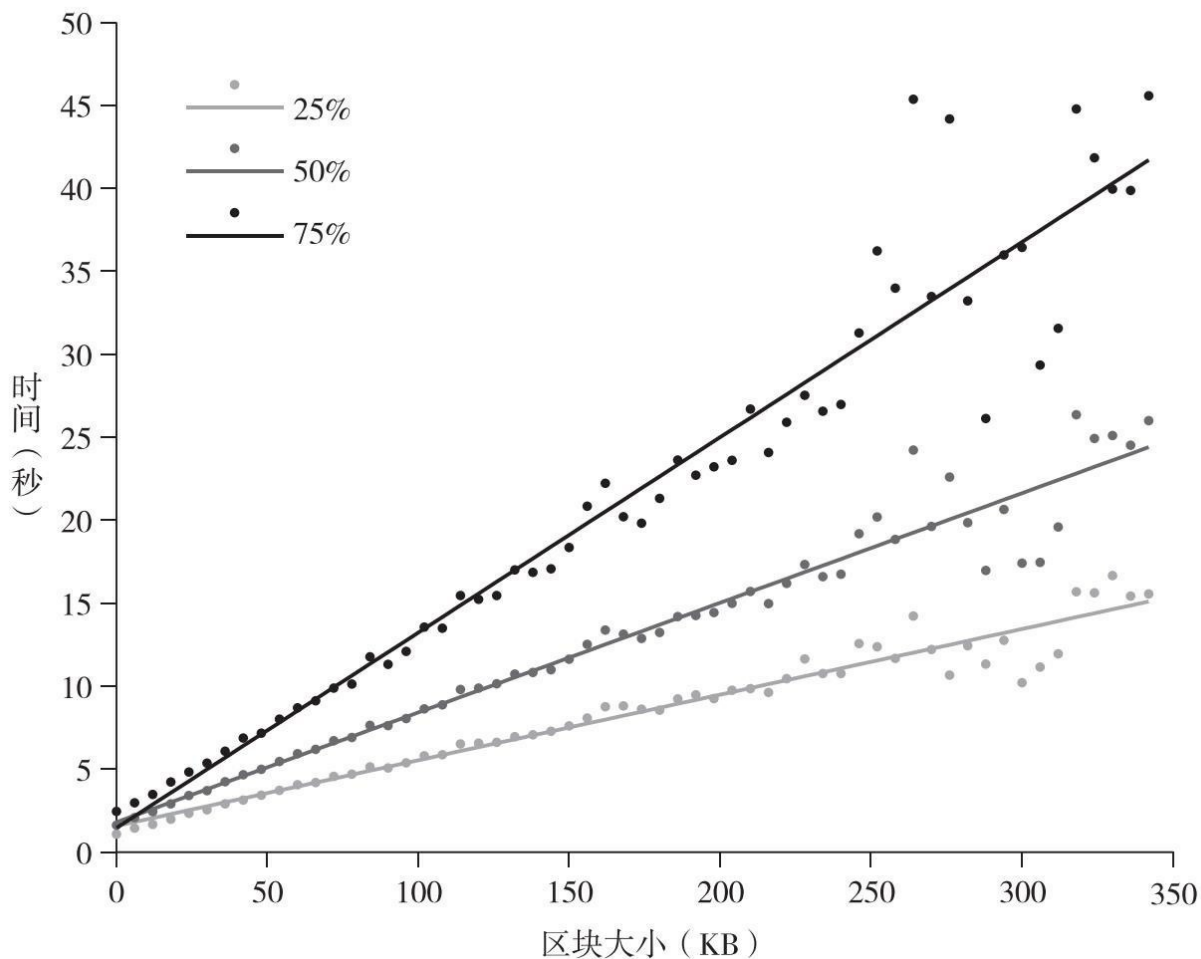


图3.9 区块传播时间

注：展示了区块被网络中不同数量（百分比）的节点接受所花费的时间。

资料来源：Yonatan Sompolsky和Aviv Zohar，加快比特币交易的传播速度（Accelerating Bitcoin's Transaction Processing, 2014）。可从下述网址获得

<https://eprint.iacr.org/2013/881>。数据由Yonatan Sompolsky和Aviv Zohar授权使用

存储空间需求

完全有效的节点必须永久在线，这样才能接收到所有的交易数据。一个节点离线时间越久，当它重新连接到网络的时候，就需要越多时间来更新所有交易。这些节点还需要把完整的共识区块链都存储下来，也需要有好的网络连接，确保可以接收到所有交易并将其转播给其他节点。目前的存储空间大约要几十个GB（见图3.10），一台台式机就能满

足要求。

最后，完全有效节点必须维护在交易中产生的（交易的输出）、未被消费掉的比特币的完整列表，这个列表最好放在内存而非硬盘里，这样，在接收到一个交易信息的时候，节点才能快速查看、运行脚本，验证签名是否有效，然后把交易放入交易池。到2014年年中，大约有4400万的交易被纳入区块链，其中有1200万个交易产生的比特币没有被使用。还好，这个数据不大，可以很容易地放进1G内存里。

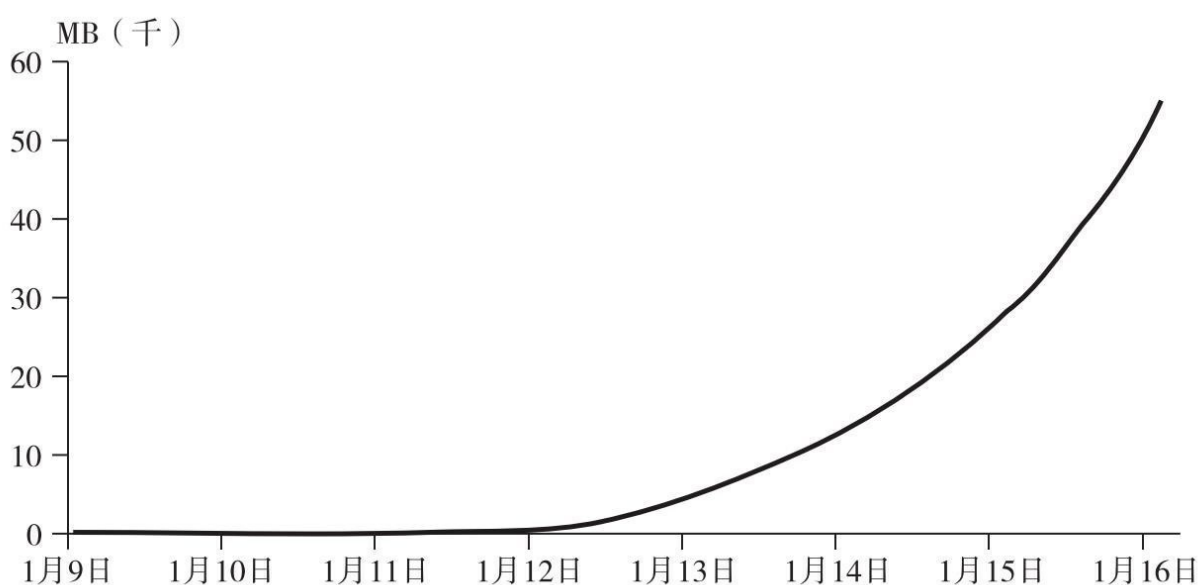


图3.10 区块链的大小

注：全节点必须保持整个区块链，在2015年年底，区块链大小在50GB以上。

轻量节点

除了完全有效节点之外，还有一种轻量节点(lightweight nodes)，或者称为轻客户端，也叫**简单付款验证**（Simple Payment Verification，简称SPV）客户端。事实上，在比特币系统里的大部分节点都是轻量节点。这些节点不会存储整个比特币区块链，它们只存储它

们所关心的、需要进行核验的部分交易。如果你使用一个钱包软件，那里面就会有一个SPV节点，这个节点只会下载向你的账户付款的交易及区块头部。

一个SPV节点的安全等级远不如全节点。它可以核验那些很难被挖到的区块——因为它有区块头部数据，但它不能核验一个区块里所有交易记录的有效性——因为它没有所有的交易历史记录，也没有那些未被消费的比特币的列表。SPV节点只验证那些和它们相关的交易，所以它们必须依赖那些全节点去验证网络上的其他所有交易。这虽然是一种安全性上的妥协，却不是个坏主意：轻量节点依赖全节点去处理那些比较难的工作，但当某个区块由于某些原因未被矿工挖出来时（挖矿成本巨大），这些轻量节点也会做一些核验来确保这个区块不会被拒绝。

作为一个SPV节点可以节省很多资源。区块头部的大小只是整个区块链的千分之一。所以轻量节点不需要几十G的存储空间，只需要几十MB即可，即使一部智能手机也能成为比特币网络的轻量节点。

比特币是一个开源协议，比特币网络一定是由实现方式各不相同的软件系统在无缝交互。这样，即使有些软件系统有缺陷，也不至于使整个比特币网络瘫痪。比较好的现象是，人们用不同的语言不断地重新实现协议，有些人用C++、有些人用Go语言，还有不少人用其他语言。不好的现象是，绝大部分的节点都会调用比特币官方客户端的资源库

（`bitcoind library`），这个库是比特币核心代码开发者们用C++开发的库，而且有些节点用的是过时的版本。所以，即使在同一时间，大家运行的客户端都略有不同。

[1] 竞态条件也可理解为紊乱情况。——译者注

3.6 限制与优化

最后我们要谈一下比特币协议的一些内在限制，以及优化的难度。在比特币2009年刚问世的时候，它的协议有许多内在的硬性限制，那是因为在那时没有人会想到它会发展成一个重要的国际货币。比如每个区块的平均时间、块的大小、每个区块的签名数目、切分性、比特币总量、区块奖励结构等。

比特币的总体数量与记账奖励很可能永远都不会改变，因为那样经济影响太大。矿工与投资人都在比特币现有的框架内投入巨资，如果这个框架改变了，会对他们产生巨大冲击。所以，社区基本达成共识，不管这些特性好或不好，都不应该改变。

但其他一些方面的改善可以让所有人受益——因为一些初始设计事后来看确实不太合理。其中最主要的是比特币系统的交易处理能力。每秒钟比特币网络到底可以处理多少交易？这个硬伤来自对区块大小的硬性规定，每个区块大小限定在1MB，每个交易大约是250字节，所以每块最多容纳4 000个交易。平均每隔10分钟，有一个矿工获得记账权利，所以每秒钟只能处理7个交易，这就是比特币网络的交易处理能力！似乎改掉这些限制只是需要改掉源代码的某些常数这么简单，实际上却并不容易，后面我们会简单分析一下原因。

比特币的交易处理能力到底属于什么水平？和前主流的一些信用卡公司相比，比特币这个处理能力实在太低了。我们可以做一下比较：维萨（Visa）平均每秒处理2 000笔交易，峰值每秒处理10 000笔交易。贝宝（PayPal）的交易处理能力比维萨弱，但峰值时每秒也能处理100笔交易。比特币无法处理这种量级的交易。

另一个限制是比特币用的密码算法。现在只有几个哈希函数算法和

一个签名算法可以使用。比特币使用的签名算法是ESDSA——一种secp256k1的椭圆曲线数字签名算法（见第1章），大家担心在比特币的一生（大家都希望是很长的一生）中，这个算法可能会被攻破。哈希函数也有同样的问题，比特币使用的SHA-1也有弱点，近10年来，对SHA-1的分析也逐步取得了一些进展（尽管并不致命）。为了改变这些问题，我们不得不加强比特币的脚本语言来支持新的密码算法。

修订协议

那我们到底怎样才能修订比特币协议并引入一些新特性呢？你也许认为这很简单，只要发布一个新版本，然后更新所有的节点。但事实上非常复杂，实际中，我们根本无法假定所有的节点都会更新版本。网络里的某些节点会无法获取新版本，或无法及时获取新版本。绝大多数节点更新了协议、部分节点没有更新的后果是否严重，取决于协议更新的内容。按照产生的结果，协议修订可以分为两种类型：一种会造成硬分叉，另一种会造成软分叉。

硬分叉

通过修订协议引入新的特性，可能会使前一版本的协议失效。即运行新版协议的节点认定为有效的区块，会被运行旧版协议的节点认定为无效。而由于我们不能确保每个节点都会更新协议，我们只能假定大部分节点已经升级（新节点），但还有部分节点没有升级（老节点），很快，最长的那个区块链分支里包含的某些区块会被老节点认定为无效区块，因此，老节点会认为其他的分支（在这个分支中，所有新节点认为有效的区块都会被排除在外）才是最长、有效的区块链分支，并一直扩展这个分支，直到它们更新了版本。

这种改变称为硬分叉，它使得原先的链分裂了。网络上的所有节点

会根据其所运行的协议版本去扩展两条不同的区块链，当然，这两个分叉再也不会合并。那些老节点只要不更新版本，就被永远地排除在了另一条链之外，这是比特币社区所不能接受的。

软分叉

另一种修订是加入新的特性，让现有的核验规则更加严格。那样老的节点依然会接收所有的区块，而新的节点会拒绝一些。这样的改变叫作“软分叉”。这可以避免硬分叉所造成的永久分裂。

我们如果引入可以产生软分叉的新版协议，会有什么后果呢？运行新版协议的节点会使用一些更严格的规则，现在，假定绝大部分节点都更新了新版协议并执行新的规则（这是产生软分叉的关键，因为老节点不会执行新规则，新节点的数量要足够多才能够竞争最长的链）。这种情况下，老节点可能会挖到一些无效的区块——因为这些区块中包含一些在新规则下无法核验通过的交易，然后，老节点会知道它们核验有效的区块不被别的节点接受（即使它们并不知道原因），这使得老节点的矿工会去更新协议。而且，如果新节点用它们的区块扩展了老节点的分支，那么，老节点也会转而扩展这个分支，原因是新节点核验通过的区块，老节点也必定能核验通过。这样就没有硬分叉了，只是会有很多临时的小型分叉而已。

本章3.2节提到的“支付给脚本的哈希值”就是软分叉的一个经典例子。第一版比特币协议里并没有P2SH。P2SH之所以造成软分叉，是因为对老节点而言，一个有效的P2SH交易也可以核验通过——它只验证这个哈希值跟前一笔交易输出哈希值是不是一样而已，它并不知道还要进一步检验脚本是否合法。我们依赖新版节点去进行这项核验：脚本本身真的可以获取到前一个交易输出的币。

那我们到底可以通过软分叉为比特币协议添加哪些特性呢？P2SH是成功的，也许添加新的密码算法也可以通过软分叉实现。我们也可以

通过软分叉在元数据的币基参数中添加更多的信息实现，目前，币基参数可以是任何数值，但未来我们也许可以限定币基参数的格式。已经有人提出，可以在币基参数里放入一个梅克尔树根，其中包含所有未被消费的比特币的信息。这种做法只会造成软分叉，因为老节点核验通过的区块，在新节点上可能无法核验通过。但随着区块链的延长，很快老版本就会转而去扩展最长的区块链分支。

其他的一些改变可能就会产生硬分叉了，比如在比特币里添加新的功能操作代码、改变区块大小和交易规模，甚至其他一些修复性的改动。本章3.2节提到过MULTISIG指令存在一个缺陷，它会推送给堆栈一个莫名其妙的值，要修复这个缺陷，也会产生硬分叉。这就是为什么尽管这个缺陷很烦人，但也一直没有修复，因为和硬分叉相比，保留一个缺陷还是可以忍受的。有些修订非常有意义，但目前比特币环境不太可能接受硬分叉。但许多优秀想法都在其他的竞争币中得到了测试而且成功运行，因为那些竞争币系统是从头开始建立的，硬分叉不会产生严重的后果。我们会在第10章进行更多的讨论。



比特币区块大小的难题

因为比特币变得越来越受欢迎，到2016年年初，已经开始经常发生区块被交易写满的情况，尤其是当区块在超过10分钟后还没有被矿工挖出来时（因为挖矿的随机性，确实有些区块在10分钟后还没有被挖到），这使得有些交易不得不排队等待被写进区块链。但要改变区块大小，就需要硬分叉。

究竟是否要改变，以及如何改变区块大小，在比特币社区里有热烈的讨论。这些讨论几年前就开始了，但一直进展缓慢，无法达成共识，近来讨论日趋激烈。我们在后面第7章会讨论比特币的社区、政治与管理。

随着区块大小问题得到共识解决方案，本章的一些细节有可能会过时。提高比特币交易处理能力的一些技术细节很有意思，我们鼓励读者可以通过网络阅读更多的资料。

到了这里，你一定对比特币的技术机制有了一定程度的了解，也知道比特币节点是如何工作的。但是我们自身并不是一个比特币节点，你不会在大脑里运行比特币节点程序。那我们到底如何和网络进行交互，从而使比特币可以成为一种货币呢？如何让一个节点通知你交易信息呢？如何使用现金来交换比特币呢？又如何储存比特币呢？对于如何创造一种可被人们使用的货币（而不仅仅是一个软件）来说，这些问题至关重要，我们将会在下一章回答这些问题。

延伸阅读

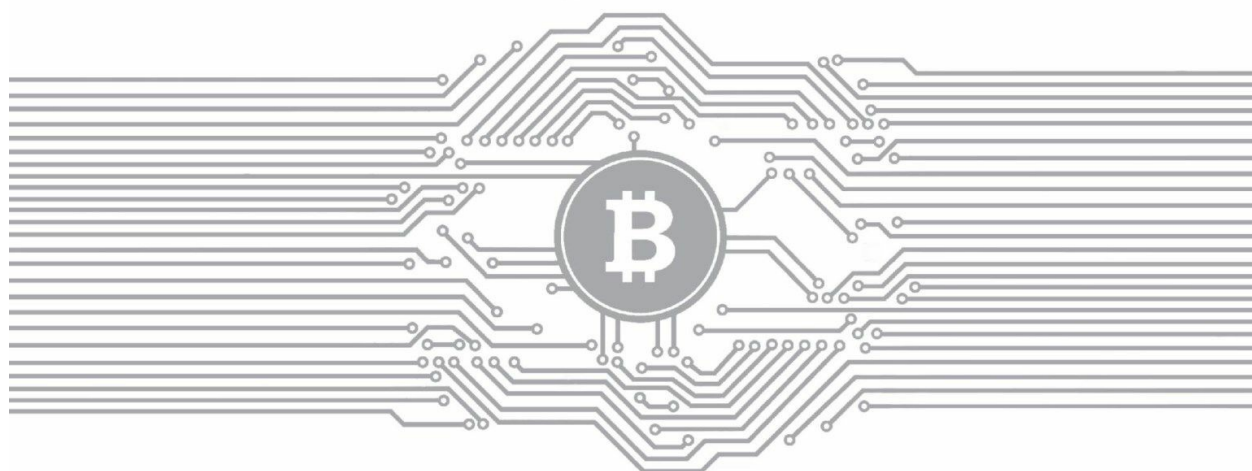
在这一章中我们讨论了很多技术细节，你也许很难一次消化。作为本章的补充读物，你可以上网查阅一些我们讨论过的资料。网上有许多网站能让你看到区块和交易到底是什么样子的。比如有一个“区块链浏览器”，网址是：blockchain.info。

还有一本比特币开发手册也很好地讲述了一些技术细节（尤其是其中的第五、第六和第七章）：

Antonopoulos, Andreas M. Mastering Bitcoin:Unlocking Digital Cryptocurrencies . Newton,MA:O'Reilly Media,2014.

第4章

如何储存和使用比特币



本章主要讨论实际应用中如何储存和使用比特币。

4.1 简单的本地储存

让我们从最简单的储存方式开始，也就是把比特币存放在本地设备上。如我们之前所说，要使用比特币，你首先要知道一些公共的信息和一些私密的信息。公共信息就是那些记录在区块链上的内容——该比特币的识别信息、币值等。私密信息即比特币持有人——也就是你本人的私钥。你不必太担心如何储存公共信息，因为你随时都可以去调取。但是私钥则是你需要好好保管的。所以在实际运用中，储存比特币就是储存与管理你的私钥。

储存比特币其实就是如何保存和管理比特币私钥。

储存与管理私钥，主要有三个目标：第一是可获取性，当你要用比特币的时候，可以随时随地取用；第二是安全性，保证没有其他人可以动用你的比特币，如果有人能动用你的比特币，那他可以直接转账给自己，之后你就不再拥有这个比特币；第三是便利性，密钥管理应当是简单易行的。你可以想到，要同时做到这三点是很不容易的：

不同的密钥管理方法就是对上述三点（可获取性、安全性和便利性）做出权衡。

最简单的钥匙管理当然是把它们储存在你自己的本地设备上：你的个人电脑、你的手机，或你持有的、拥有的或控制的小玩意。用智能手机应用软件，按几个键你就可以支配使用你的比特币了，这么做的确非常方便。但这样做的可获取性或安全性都不是很好，如果你的设备丢失，或者你的设备死机，你需要格式化你的磁盘，或者你的文件被病毒

侵蚀，你的私钥就丢失了，你的比特币也就一同丢失了。安全性方面的问题是类似的，例如有人窃取你的设备或入侵你的设备或者让你的设备中毒，将你的私钥拷贝，这样他们就可以将你所有的比特币转给他们自己了。

换言之，将私钥存储在你的本地设备，尤其是手机设备，就好比你将钱放在你的钱包里。在日常花销的时候是很方便，但你一定不想将你的毕生积蓄都带在身边，因为你不想遗失或被盜。所以一般而言，你只把一小部分信息——一小部分钱放在你的钱包里，而把你大部分钱存在其他地方。

比特币钱包软件

如果你想本地存放比特币，一般都会使用比特币钱包软件，也就是一个管理你的比特币和私钥信息并让你方便使用的一个应用软件。例如你想花相当于4.25美元的比特币在咖啡馆买杯咖啡，这个钱包应用应该很容易让你做到。比特币钱包非常有用，尤其是你需要处理一大堆地址和与其相关的密钥的时候。前面说过，制定一对公钥私钥很容易，你可以用其来匿名与保护你的个人隐私。钱包应用就是这样一个简单的接口，告诉你钱包里有多少比特币。当你要使用比特币的时候，它会处理关于密钥管理的一切技术细节，比如使用密钥或生成新的地址等。

编码解码（encoding keys）：Base58编码和二维码

要使用或是接收比特币，你需要与对方交换地址——比特币送达的地址。目前有两种主流的方式将地址加密：一种是字符串，另一种是QR（Quick Response）码^[1]。

为了给地址赋予一个字符串，我们把密钥的字节从二进制字符转换成Base58码。Base58就是用一个包含58个字符的字符集来编码，这被称为base58记号法。为什么是58个字符？我们把大写小写字母都算上，然后去掉几个比较容易混淆的字母，比如大写的“O”与“0”看起来很像，就得到了58个字符。我们可以将加密的地址读出来，或者在需要时也能够打印出来。理想情况下，最好能避免这种手工的方式，而是采用其他方法，例如我们接下来要讨论的QR码。

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

以上就是比特币创世块地址的Base58代码。



图4.1 QR码

注：一个QR码代表着一个真实的比特币地址。请扫上面的QR码给我们转账一些比特币。

第二种方法是用QR码，一种简单的二维码。用QR码的好处是你可以用手机拍张照片，然后钱包应用会把QR码自动转换成代表比特币地址的字节。这对商店十分有用：比如一个付款机可以显示一个QR码，你可以用手机扫描一下，然后就可以用手机把比特币转账到付款地址。这对于手机与手机之间的转账也很有用。

虚荣地址

有些商家或个人喜欢将地址转换成一些人能够识别的字符。例如，博彩公司网站中本聪骨头（Satoshi Bones）的收款地址中就含有“骨头”（bones），如下所示的2—6位字符

（1bonesEeTcABPjLzAb1VkFgySY6Zqu3sX），当然所有的地址都是1开头的，代表支付到比特币地址的标准交易或者说是标准的比特币转账流程（pay-to-pubkey-hash）。

地址都是通过哈希计算产生的随机字符串，那么如何才能获得含有“bones”字符串的地址呢？如果中本聪骨头只是随便制定它们的地址，无法进行逆向计算哈希函数，它们无法得到相应的私钥，也无法控制地址的生成。这样的话，它们只能不停地重复生成私钥，直到私钥中包含它们希望出现的字符串。这样的地址被称为**虚荣地址**（vanity address）。这种地址事实上是可以通过工具生成的。

一般需要多少工作量能得到这样的结果呢？由于每个字符位有58种可能性，如果你想得到一个字符串中有k个字节的特殊字符，你平均需要生成58的k次方地址，才能获得你要的结果。所以如果要生成“bones”开头的地址则要生成超过6亿个地址！这个工作现在通过一台笔记本电脑就可以完成。但是你每增加一个字符，工作量会几何级数增长。获得一个15位字符的地址需要的计算量难以想象，而且是不间断的哈希计算，这是无法实现的。



虚荣地址的加速生成

在比特币世界，如果我们将一个私钥称为 x ，公钥是 g^x ，其地址是 $H(g^x)$ ，即公钥的哈希值。我们不会探讨其中的细节。但是通过指

数运算来生成地址显然是很慢的。

最直接的方式是挑选一个伪随机序列 x ，计算 $H(g^x)$ ，不停地生成地址，直到得到想要的结果为止。一个更快的方式是，如果使用 x 无法得到想要的结果，接下来就使用 $x+1$ 来计算，如此反复。而不是重新挑选一个 x 。因为 $g^{x+1} = g \cdot g^x$ ，而我们已经计算过了 g^x ，所以我们只需要做乘法运算而无须做指数运算，这会更快。事实上，这种方式比最直接的方式要快两个数量级以上。

[1] QR码是一种简单的二维码。——译者注

4.2 热储存与冷储存

如我们所看到的，把比特币放在你的个人电脑里就像把钱放在钱包里带着，这叫“热储存”。这很方便但很不安全。而另一方面，“冷储存”是离线的，把比特币锁在其他地方。冷储存不联入互联网，是封存起来的。所以相对安全和保险，但是很显然不方便。这就像你带着一些零钱出去，但是把终生积蓄锁在保险箱里的道理一样。

要分开热储存和冷储存，你也必须要用不同的私钥，否则如果热储存被人破坏了，冷储存也会处于危险之中。你也需要把币在两边转来转去，这样两边都需要知道对方的地址或公钥。

因为冷储存是离线的，所以热储存与冷储存无法通过网络相连，但其实冷储存不需要上线就可以接收比特币——热储存端知道冷储存的地址，所以它随时可以给冷储存转账。当你觉得你的钱包里的钱太多的时候，你可以把一部分的币转到冷储存，但不需要让冷储存上线而暴露自己。当然，只要冷储存上线，就可以接收到区块链的转账信息，然后可以随意处理这些比特币。

但管理冷储存有一个小问题：一方面，为了私密性和其他考虑，我们希望使用不同的地址（这些地址有不同的密钥）收款。所以我们把比特币从热储存转到冷储存的时候，要用一个新的冷储存地址。但是由于冷储存不上线，所以热存储端必须要能找到这样的地址。

一个直接的解决方案是让冷储存一次性生成一批地址，然后把地址列表发送给热储存，热储存可以依次使用这些地址，当然，这个方法的缺陷是为了传送地址，我们不得不经常让冷储存端上线。

分层确定性钱包

一个比较有效的解决办法是使用一个分层确定性钱包（**hierarchical deterministic wallet**）。这个方法可以让冷储存端制造无限制的地址数量，然后通过一个短暂的、一次性的交换，让热储存端知晓所有地址。但这需要使用密码学的技巧。

回想一下，我们在第1章谈到密钥生成和电子签名时，我们使用了“**generateKeys**”来生成一个公钥（也就是地址）和一个私钥。在分层确定性钱包里，生成密钥的方式不太一样。不同于生成一个单一地址，我们生成一个被称为“地址生成信息”的东西；我们也不只生成私钥，而是生成“私钥生成信息”。有了地址生成信息，我们就可以生成一系列地址。我们把地址生成信息和一个整数*i*作为地址生成函数的输入参数，就生成了序列里的第*i*个地址。同样，我们用私钥生成信息来生成一系列私钥。

密码学的神奇之处在于：对于每个*i*而言，第*i*个地址和第*i*个私钥相匹配——换言之，第*i*个私钥控制第*i*个地址的比特币，就好像这是用经典办法产生的。这样一来，我们就有一长串配对的公钥和密钥。

密码学的另一个技术优点是安全性——地址生成信息并不会泄露关于私钥本身的任何信息。这意味着你可以放心地把地址生成信息给任何人，他就可以用它来生成第*i*个密钥。

并不是所有的电子签名算法目前都可用于生成分层确定性密钥。比特币使用的电子签名算法ECDSA支持分层密钥，让我们可以使用这个技巧。即冷储存端生成任意多个密钥，热储存端生成相应的地址，见图4.2。

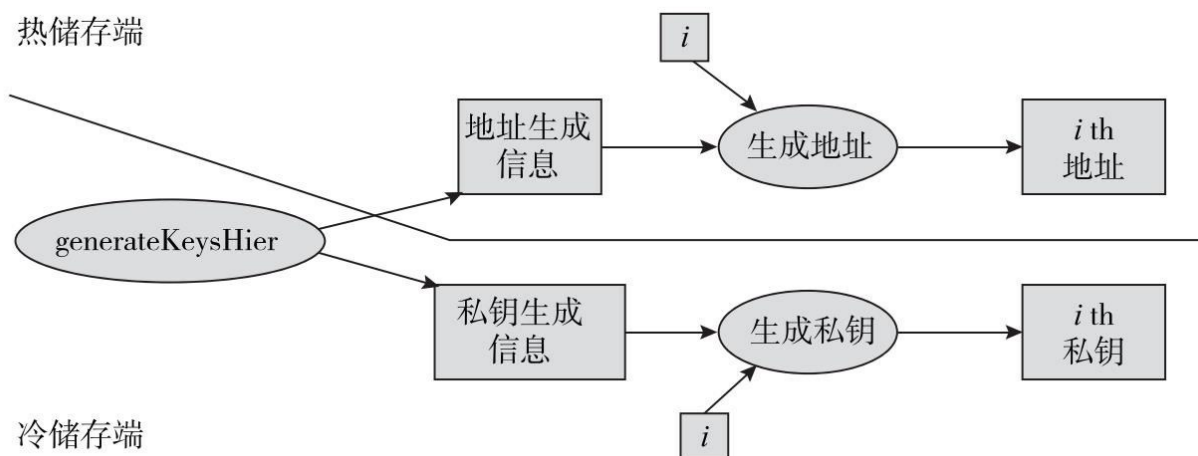


图4.2 分层确定性钱包示意

注：冷储存端生成和保存私钥生成信息和地址生成信息，然后将地址生成信息一次性转给热储存端。当热储存端要给冷储存端转账时，就按次序生成新的地址。冷储存端上线后，也会按顺序生成地址，然后查收相应地址收到的款项，直到某一地址没有收款位置。如果冷储存端需要向热储存端转账，它就会按顺序生成私钥序列。

ECDSA的工作机制如下：通常一个ECDSA私钥是一个随机数 x ，其对应的公钥是 g^x 。为了生成分层确定性密钥，我们需要另外两个随机数 k 和 y 。

私钥生成信息： k, x, y

第 i 个私钥： $x=y+H(k \parallel i)$

地址生成信息： k, g^y

第 i 个公钥： $g^{x_i}=g^{H(k \parallel i)} \cdot g^y$

第 i 个地址： $H(g^{x_i})$

分层确定性钱包有我们需要的所有特性：两方都可以生成公钥/私钥序列，而且这些公钥/私钥相互配对（因为与私钥 x 对应的公钥就是 g^x ）。而且，这种方法还具有另外一种我们尚未提及的特性：当你向外提供这些公钥时，这些公钥之间没有联系，也就是说，别人无法断定这

些公钥来自同一个钱包。稻草人方案（冷储存端生成大量的地址）也具有这种特性，但我们需要小心地保护这些地址，因为这些地址事实上并不是独立生成的。这种特性对于保护隐私和实现匿名是至关重要的，我们将在第6章展开讨论。

分层确定性钱包有两种不同的安全性，热储存端的安全性较低。如果热储存受到损害，那么上文提到的非相关性就不复存在，但这种情况下，私钥（以及比特币）仍然是安全的。通常，分层确定性钱包支持任意多个安全等级——这也是“分层”的由来——虽然，我们还没有讨论细节。这种安排非常有用，例如，当一家公司内部存在多种授权级别时，就需要这种特性。

现在，我们讨论一下冷储存如何保存信息（私钥或私钥生成信息）。第一种方式是将信息保存在某个设备（例如笔记本电脑、手机或平板电脑，或U盘）中，然后将这个设备好好保管，最好是让这些设备断开网络，并将其锁起来，这样，如果有人想盗取信息，那么他首先需要进入这些设备的保存处。

大脑钱包

第二种方法我们称之为**大脑钱包**（brain walle）。这种方式下，你通过一个密码就可以支取比特币。大脑钱包无须使用硬件、纸张或者其他长期储存介质。大脑钱包在物理安全性较差的情况下（例如跨国出差、旅行时）非常有用。

大脑钱包的主要原理是用一个可预测的算法把一个口令变成一对公钥/私钥。例如，你可以选择一个哈希算法将口令转译成一个私钥。在给定私钥的情况下，可以用同样的方法得到私钥。进一步地，结合前文所提到的分层确定性钱包技术，你可以根据口令生成一整套地址和私

钥，从而实现钱包的完整功能。

但是，如果一个黑客猜到你的口令的话，他还是可以偷走你大脑钱包里的所有私钥。在电脑安全领域里，我们通常假定黑客知道你生成密钥的步骤，黑客不知道的只是你的口令。所以黑客可以尝试使用不同的口令，生成地址，并在区块链中查看这些地址上是否还存在未被使用的比特币，一旦发现比特币，黑客就可以迅速把这些比特币转给自己。黑客可能永远都不知道（或者根本不关心）这些比特币属于谁，这类攻击也不需要入侵任何设备，猜口令不针对任何人，所以也不会留下任何痕迹。

这种方法与尝试破解电子邮箱密码的方法不同，邮件服务器通常对密码试错有一定的次数或频率限制（被称为在线猜测），但是对于大脑钱包而言，黑客可以下载一堆未被使用的比特币的地址，然后用电脑程序去慢慢地试错，黑客都不需要知道大脑钱包的地址，这被称为离线猜测或者密码破解。相应地，设置口令的难度大大增加了，又要容易记，又要不容易被猜中。一种安全的方法是使用自动程序生成一个80位的数字，然后将其转换成口令。



生成一个可记忆的口令

有一种简便的方法可以生成口令：从最常用的10 000英语词汇中，随机选择6个词，从而生成大致80位长度的字节[$6 \times \log_2(10\ 000)$ 大致等于80]。很多人发现这个方法比随机取字母容易记忆，因为这种方法生成的口令通常是下面这样子的：

worn till alloy focusing okay reducing
earth dutch fake tired dot occasions

在实际操作中，我们可以让程序生成密钥的速度变慢（为程序加入一个延迟），这样，黑客通过试错法来破解私钥就需要花费很长的时间，这就是所谓的密钥延展（key stretching）。比如，为了使密钥生成变慢，我们可以让程序把本来很容易计算的哈希函数SHA-256算上 2^{20} 次，这样一来就把黑客的工作量增加了 2^{20} 倍。当然，如果太慢的话，用户在使用比特币的时候，也会计算得很慢，这也很麻烦。

如果你彻底忘记了大脑钱包的口令，钱包里的比特币就永远取不出来了。

纸钱包

第三个选择是纸钱包（见图4.3）：把密钥印在纸上，然后把纸锁在保险箱里。显然，这种方式的安全程度取决于我们所使用的纸的安全程度。纸钱包通常用两种方法为公私钥匙编码：二维码和base58码。就像大脑钱包一样，只需要存储少量关键信息，就可以重新建立一个纸钱包。

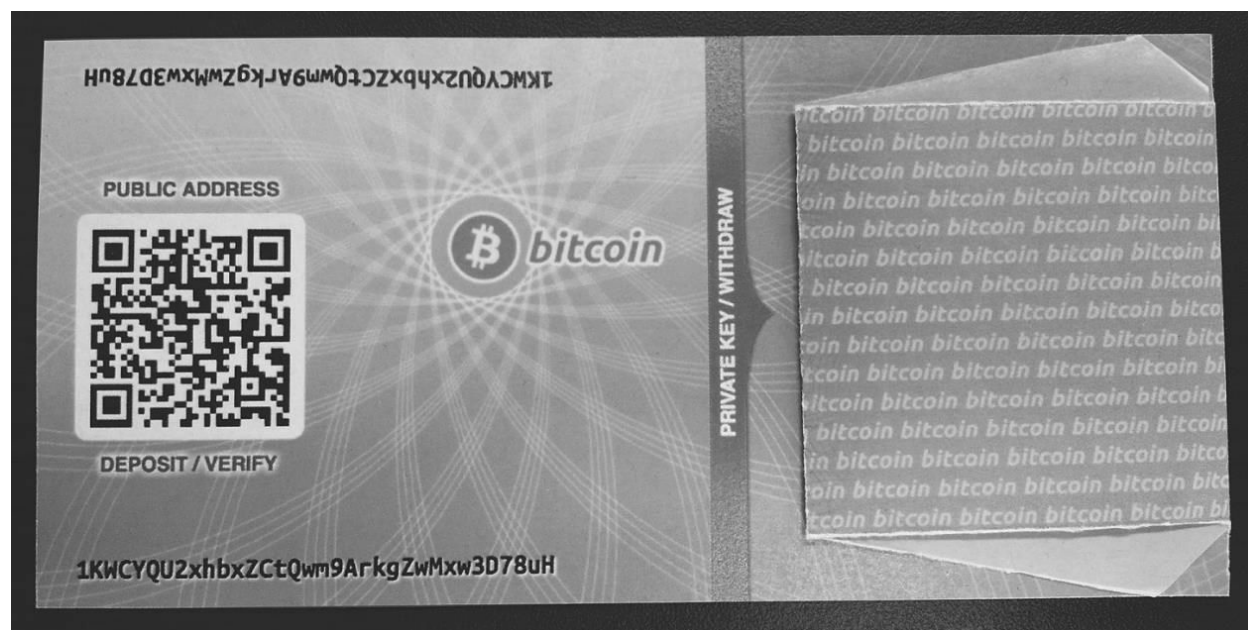


图4.3 带公钥的比特币纸钱包

注：同时使用了二维码和base58码加密。

防损硬件

第四种方法是使用防损硬件（tamper-resistant device），用它来保存密钥或用它来生成密钥，总之，此类设备本身不会泄露密钥或输出密钥，而只是在我们按下设备的某个按钮或输入设备密码后显示密钥的保管状态。防损硬件的好处在于一旦设备丢失或者被盗，我们马上就能知道。而且，想要盗走密钥，必须先盗走这个设备。这和将密钥保存在电脑上是不一样的。

总而言之，用户可使用上述一个或是多个方法来保存密钥。对于热储存，尤其是存有大量比特币的热储存而言，人们愿意投入大量成本或先进的安全机制保护它们。我们将在下一章讨论这些更先进的机制。

4.3 密钥分存和密钥共享

现在我们了解了各种保存密钥的方法，但在这些方法里，我们总是把密钥保存在一个地方：要么锁在保险箱，要么保存在软件中或打印在纸上。这会造成一个问题：一毁俱毁。当然，我们可以为密钥建立备份，这可以降低密钥丢失或损坏的风险（可获取性），但同时会增加密钥被盗的风险（安全性）。那是否存在一种方法，可以使密钥的可获取性和安全性都得到提高？答案是肯定的。密码学上有一种称为“密钥分存”的技术，就可以做到这一点。

方法如下：密钥被分成N个片段，只要我们获得其中的K个片段，就可以把原密钥重新还原。但如果获得的片段数量少于K，就无法知道关于密钥的任何信息。

要实现上述效果，把密钥简单地切分成若干片段是不行的，这样的话，每一个片段都会透露密钥的部分信息。^[1]所以，密钥分存并不是简单地切分密钥，而是将密钥转换成若干“子密钥”。

举个例子，我们设定 $N=2$ ， $K=2$ ，意味着我们把想要加密的密钥（原密钥）转换成两个子密钥，只有同时获得这两个子密钥才能拼出原密钥。我们把原密钥称为 S ， S 是一个很大的数字（比如128位）。然后，我们可以随机产生另一个128位的数字 R ，让 R 作为其中的一个子密钥，那么另外一个子密钥就是 $S \oplus R$ （ \oplus 代表逻辑算符互斥，exclusive OR，或缩写成XOR，也叫异或），我们把 $S \oplus R$ 称为“密文”。然后，我们把子密钥 R 和密文 $S \oplus R$ 保存在两个不同的地方。单独根据子密钥 R 或密文都无法知晓原来密钥的任何信息，但如果我们同时得到 R 和 $S \oplus R$ ，我们可以通过异或逻辑运算得到原来的密钥。^[2]

N和K相等时，我们总是可以这样做：对于之前的K-1个子密钥，我们可以生成N-1不同的随机数，最后一个子密钥就是原密钥与所有其他N-1个子密钥的异或。但如果N大于K的话，这个技巧就行不通了。我们需要借助其他代数方法。

图4.4中，我们是如何生成子密钥的呢？首先，我们把S标记在Y轴上 $(0, S)$ ，然后经过该点画一条直线，斜率随机，接下来，我们就可以在这条线上挑一些点，要多少有多少。这样，我们就得到N个子密钥，并且 $K=2$ 。

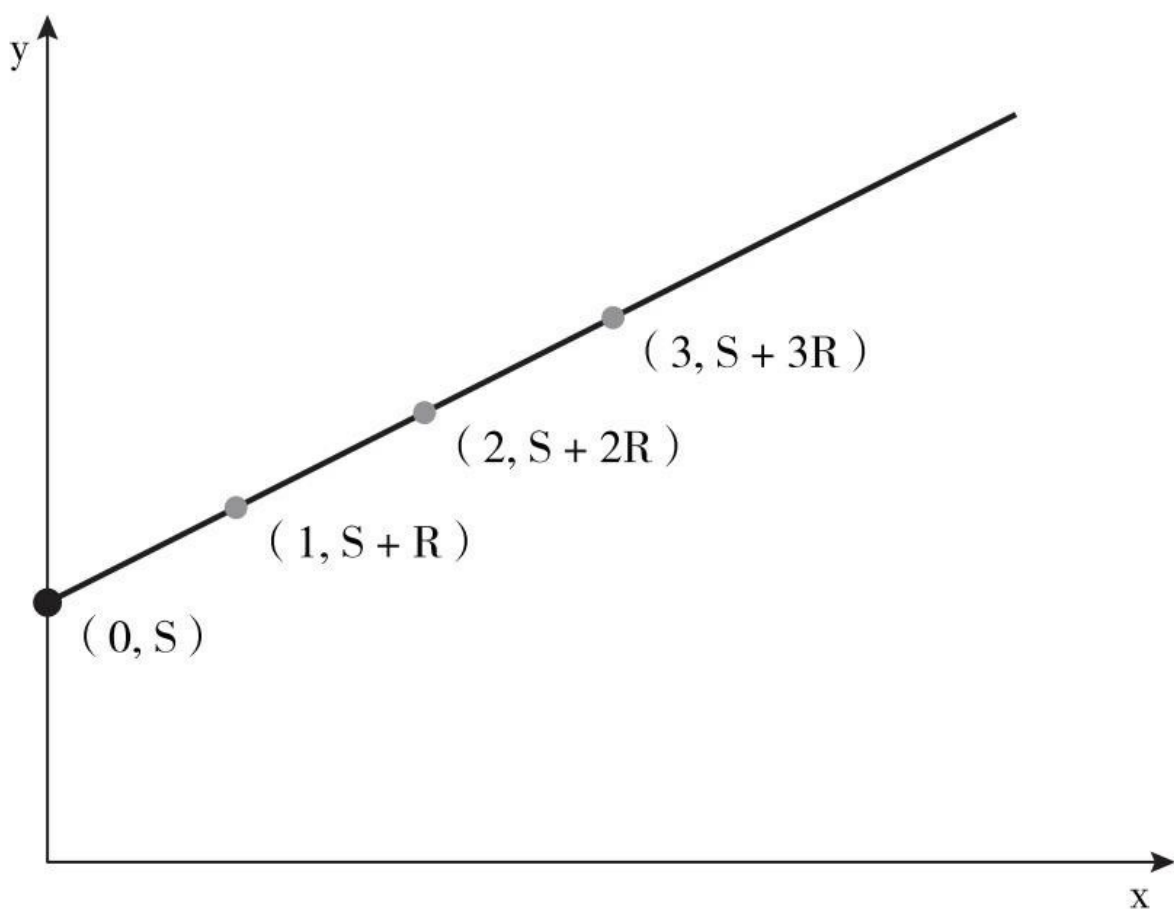


图4.4 密钥分存的几何示例 ($N=2$)

注：S代表原密钥，被编码成一个大的整数，图中斜线的斜率随机。斜线上的点（主要是它们的Y坐标 $S+R$ ， $S+2R$ ， \dots ）代表子密钥。连接任何两个点，都可以得到S[两点连线，延长，与Y轴的交点就是S（黑点）]。若是只有一个点，又无法确定斜率（斜率随机），就无法得到S。

为什么我们得到两个点就可以还原原密钥呢？首先，连接两个点可以得到一条直线，这条直线和Y轴的交点就是S。然而，如果只有一个点，将得不到任何信息，由于直线斜率是随机的，所以，通过该点的任何直线都有可能是我们生成子密钥所采用的那条直线，但所有直线和Y轴的交点都不同。

上述方法中，有一点很精妙：要让这个方法在数学上行得通，我们需要找一个足够大的素数P取模。P不需要和原密钥有任何关系，只需要足够大就可以。S的值在0和P-1之间（含0和P-1）。上文中，我们说通过S画直线并在直线上挑选一些点，实际操作时，我们其实是生成一个介于0到P-1的随机数R，并生成下列点：

$$x=1, y=(S+R) \bmod P$$

$$x=2, y=(S+2R) \bmod P$$

$$x=3, y=(S+3R) \bmod P$$

原密钥对应的坐标为 $x=0, y=(S+0 \times R) \bmod P$ ，其实就 $x=0, y=S$ 。

上述方法在 $K=2$ ，N为任意数字的情况下都有效，例如，如果 $N=4$ ，就是生成4个子密钥，并保存在4个不同的设备里。万一有人偷了其中的一个，他对密钥仍一无所知。即使丢了两个子密钥，你也仍然可以通过另外两个子密钥来得到原密钥。

上述方法可以进一步扩展：我们可以用任何的K和N（只要保证 $K < N$ ）来实现密钥分存。在图4.4中我们用一条直线进行密钥分存，在代数中，直线就是自由度为1的多项式。如果 $K=3$ ，我们就要用抛物线来实现，抛物线是自由度为2的多项式。我们可以用表4.1中所示公式来表达这一递进系列。

表4.1 密钥分存的数学原理

公式	自由度	形状	随机参数	还原原密钥所需的子密钥数量
$(S + RX) \bmod P$	1	直线	R	2
$(S + R_1 X + R_2 X^2) \bmod P$	2	二次曲线	R_1, R_2	3
$(S + R_1 X + R_2 X^2 + R_3 X^3) \bmod P$	3	三次曲线	R_1, R_2, R_3	4

注意，如果使用自由度为 $k-1$ 的曲线上的若干点来进行密钥分存，那么，为了还原原密钥，至少需要得到 K 个点的数据。

数学上，拉格朗日公式表明，如果要回归一条自由度为 $k-1$ 的曲线，需要获得至少 K 个点。最简单的例子就是，用尺子连接两个点，就可以得到一条直线。因此，如果我们将原密钥转换成 N 个子密钥，除非黑客获得了 $K-1$ 个子密钥，否则原密钥就是安全的，换个说法，我们最多可以承受 $N-K$ 个子密钥被泄露。

当然，密钥分存并不是比特币的专用技术。你可以将你的密码进行密钥分存，然后把子密钥告诉你的朋友，或把它们放在不同的地方。但是，实际上并不会有人真的这么做。一方面这么做不太方便，另一方面，目前市场上也有其他的安全机制，例如使用短信进行双重验证。但对于比特币而言，如果你选择本地保存密钥，那么双重验证等安全机制就不适用了，我们无法通过短信验证码的方式来控制比特币账户。当然，在线钱包则不同，我们会在下一节讨论。不过，在线钱包和本地储存的区别不大，类似的问题总是存在，只不过换了一种方式。毕竟，在线钱包的服务商在保存密钥的时候也不能只使用一种安全措施。

门限密码（threshold cryptography）

密钥分存还是有一个问题：密钥分存之后，如果我们后面要用原密钥来签名，那就需要取得子密钥，还原成原密钥，然后才能签名。这个

过程有可能被黑客乘虚而入，盗取密钥。

密码学可以解决这个问题。如果子密钥储存在不同的设备中，可以去中心化的方式还原原密钥，而不是在某台设备上完成。这种技术叫“门限签名”（threshold signature）技术。典型的例子就是使用双重安全机制的电子钱包（ $N=2$ 且 $K=2$ ），如果两个子密钥分别保存在个人电脑和手机上，你可以在电脑上发起付款，这时，电脑会生成一个签名片段，并发送到你的手机上，然后，手机会提示你付款信息（包括收款人、金额等），然后等待你确认。如果你确认了付款信息，这时，手机会利用它的子密钥完成整个签名，然后广播到区块链上。万一黑客控制了你的电脑，试图把比特币转到他的账户，你根据手机上的付款信息就知道有问题了，从而不会确认这笔交易。门限密码涉及的数学细节比较复杂，此处我们不展开讨论。



门限签名

门限签名是密码学中的一项技术，将一个密钥切分成不同片段，分别储存，在交易签名时无须还原原密钥。而多重签名是比特币脚本的特性，把一个比特币账户的控制权交给多个密钥，这些密钥共同保障账户安全。门限签名和多重签名都能克服密钥单点保存的缺陷。

多重签名

还有另外一种方法可以克服密钥单点保存的缺陷，即多重签名（multisignatures），这个名词在第3章曾出现过。通过比特币脚本，可

以直接把一个比特币账户的控制权交给多个密钥，而不是将密钥分存。这些密钥可以保存在不同的地点，并分别生成签名。当然，最终完成的交易的信息还是会保存在某台设备上，但即使黑客控制了这台设备，他所能做的也只不过阻止这个交易被广播到整个网络上去。没有其他设备参与，他无法生成出一个正当有效的多重签名。

举例来说，假设本书的作者安德鲁（Andrew）、阿尔文德（Arvind）、爱德华（Ed）、约什（Joseph）和史蒂文（Steven）是一家公司的创始人——也许我们就是依靠出售这本书的版权来创建公司——那这家公司就有许多的比特币了。我们可能会用多重签名来保护这些比特币。我们5个人，每人都有一对密钥，我们可以用其中的3个签名来保护冷储存——一笔交易需要5个人中至少3个人的签名才能完成。

这样，只要我们5个人在不同地方且使用不同的安全措施保存各自的密钥，那么比特币就会相当安全。黑客必须盗取我们当中3个人的密钥，才能盗取比特币。即便我们其中一个或两个背弃了我们，他（们）也无法卷款而逃，因为他们还需要另一个签名。^[3]同时，如果我们其中一个遗失了密钥，其他人还是可以取出比特币，并转到新的账户，重新设置密码。总而言之，多重签名可以比较妥善地管理在冷储存端的大额比特币，任何重大事项都需要多人的参与才能实现。

上文中，我们说到，人们使用门限签名技术的原因是为了实现双重安全机制或多重安全机制，使用多重签名技术的原因是为了实现多人对共同财产实现共同控制。实际上，这两种技术都可以实现上述两种目的。

^[1] 《鹿鼎记》里的藏宝图储存方法在现实中是不可取的，因为不需要搜集齐八旗手中的碎片，只需要有几旗的就可以猜出整个藏宝图。——译者注

^[2] 在密码学中，上文的“原密钥”通常称为“明文”，“R”称为“密钥”， $S \oplus R$ 称为“密文”。——译者注

^[3] 用这个方法倒是可以防止银行工作人员卷款而逃，可见科技的进步确实可以改善传统行

业的一些薄弱环节。——译者注

4.4 在线钱包和交易所

我们已经讨论了自己储存和管理比特币的不同方法。下面，我们将讨论如何通过他人提供的服务实现上述目的。最直接的方法是使用在线钱包。

在线钱包

在线钱包和随身带的钱包一样，只是在线钱包的信息储存在云端，你可以通过网页或手机应用来读取。2015年年初，比较流行的在线钱包服务是比特币基地公司（Coinbase）和区块链信息公司（blockchain.info）。

从安全性的角度考虑，最关键之处在于网站不仅在你的浏览器或手机应用软件（APP）上运行代码，而且，网站还储存着你的密钥。至少，网站是能够接触到你的密钥的。通常情况下，网站使用密码来保护密钥，而密码只有你一个人知道。当然，你需要信任这个网站，相信它不会泄露你的密钥或是密码。

在线钱包的一大优点是方便。你不需要在电脑上安装任何软件就可以使用在线钱包；在手机上，你只需安装一个手机软件就可以使用钱包，而且，不需要下载区块链。在线钱包可以在各种设备上使用：无论是个人电脑还是手机，因为真正的钱包信息储存在云端。

但是，在线钱包也有安全隐患。如果网站或者是网站工作人员有恶意，那么在线钱包中的比特币就有危险。在线钱包的服务器运行着所有的代码，很容易窃取你的比特币，在线钱包服务提供商如有恶意，情况

就不妙了。

通常情况下，网站或者服务提供商由训练有素的网络安全专家运行。他们比我们更专业，所以我们会认为他们帮我们保管比特币会更安全。但归根结底，前提是专家们不会故意搞破坏。

比特币交易所

要想理解比特币交易所，我们先要讨论一下传统的银行是如何运作的。你给银行一笔钱——做一笔存款，银行日后会按照你的要求把钱还给你。当然，银行并不会把你的钱一直锁在保险柜里，银行只是答应，当你提款的时候把钱给你，在这期间，银行通常会把钱用于投资。许多银行会保留一部分钱作为储备金，保证人们来提款的时候，有足够的现金。很多银行通常按存款的固定比例来留存储备金。

现在来谈比特币交易所。至少在用户使用的角度看，比特币交易所和银行很像。交易所可以办理比特币存款，日后需要用钱的时候，可以到交易所提款。你还可以把法定货币（法币）——例如美元、欧元等存到比特币交易所，交易所承诺日后会按照你的要求把钱——比特币或法币，或两者都有——还给你。也可以通过交易所办理类银行业务，例如，用比特币付款或收款。还可以通过交易所把比特币兑换成法币，或把法币兑换成比特币，交易所在该业务中通常起撮合作用，它们同时寻找愿意兑换法定货币和愿意兑换比特币的人，并安排他们作为交易对手，如果交易对手对于汇率达成一致意见，交易所就促成这笔交易。

举个例子，假设你在某交易所的账号里有5 000美元和3个比特币。你想用580美元/比特币的价格买两个比特币，这时交易所帮你找到交易对手并促成交易。现在，你的账号里有5个比特币和3 840美元。

值得注意的是，当你在交易所完成上述交易的时候，区块链上并不

会记录任何交易。交易所不需要在区块链里把比特币从一个地址转到另一个地址。交易所只是修改了你的合约，交易前，它说“我们日后会还给你5 000美元和3个比特币。”交易完成后，它说“我们日后会还给你3 840美元和5个比特币。”所以，交易前后，比特币并没有真正在区块链中移动，只是你和银行的合约变化了而已。对于你的交易对手而言，也是如此。

交易所所有优点也有缺点。优点之一是交易把比特币经济和法币经济结合起来，这两种货币实现了自由转换。如果我账户里有比特币和美元，我可以随心所欲将比特币换成美元，或把美元换成比特币，这是相当方便的。

缺点就是风险。交易所面临和银行一样的风险，主要包括以下三大类风险：

三类风险

第一类风险是挤兑。挤兑就是大家同时都去银行提款。由于银行一般只保存部分存款，所以可能无法应付所有的提款要求。当银行无法兑现的谣言四起之时，大家开始恐慌，然后更多人去银行取钱，造成崩塌效应。

第二类风险是银行本身可能就是一个庞氏骗局。庞氏骗局的通常做法就是不断借新还旧，从储户吸收存款，答应日后提供一定的收益，但实际上这笔钱并没有用于投资，而是用于支付先前储户的收益，这类骗局最终必然会崩溃，使人们损失惨重。2008年的麦道夫骗局就是庞氏骗局的最新案例。

第三类风险就是黑客入侵。有人——有的甚至就是交易所的雇员——试图入侵交易所的安全系统。由于交易所储存大量密钥，而这些密

钥可以支取比特币，所以交易所需要非常小心地监控软件的安全性及其操作流程——例如，如何管理冷热储存等。如果某个环节出了差错，我们存在交易所的比特币就会被盗取。

上述风险都实际发生过。有的交易所因为挤兑而倒闭，有的交易所因为管理员的监守自盗而倒闭，也有的交易所因为黑客入侵而倒闭。实际上，统计数据并不令人乐观。2013年的一项研究显示，40家比特币中有18家由于存款到期无法兑付或其他问题而倒闭。

倒闭的交易所中，最有名的就是门头沟（Mt.Gox）。门头沟曾经是世界上最大的比特币交易所，最后因存款到期无法兑付而宣告倒闭，许多投资者血本无归。门头沟现在还在日本与美国法院走破产清算程序，人们到现在都没有搞清楚他们的钱到底去了哪里。我们只知道一点：门头沟曾经拥有很多比特币，而现在已经一无所有了。这对于所有交易所都是一个警示。

反观传统银行业，并没有高达45%的破产率。政府的监管在其中发挥了重要的作用。政府对银行的监管主要体现在以下方面：

银行监管

政府首先要求银行有一个最低准备金要求。在美国，银行随时要保留总储蓄量3%~10%的现金来应付突发的提款请求。政府通常还会对银行的投资类别以及资金管理方法进行监管，政府要求银行的资产投向低风险资产，因为这些钱大多是储户的血汗钱，而不是银行自有的资金。

政府不仅仅对银行进行监管，还会在必要时为银行或储蓄者提供保护。首先，政府会提供储蓄保险。如果一个遵纪守法的银行破产，政府会偿还储户一部分存款。其次，政府有时候也会充当“最后借款人”角色。如果银行短期经营困难，但仍有一定的偿债能力，政府给银行提供

贷款，直到银行有足够的资金周转，从而让银行渡过难关。

传统银行的监管大抵如此，但比特币交易所的监管则并非这样。比特币交易所需不需要被监管，我们会在第7章讨论。

准备金证明

比特币交易所或者其他提供比特币管理服务的机构，可以使用一种称为“准备金证明”（proof of reserve）的密码学技术来向储户证明他们留存了一部分储备金——例如，按照储蓄额的25%留存——从而消除投资人的担心。

准备金证明包括两方面的内容：首先是证明你有多少准备金。这比较容易，交易所只需发起一笔向自己转账的交易，转账的金额等于其公布的准备金金额即可。如果交易所声称留存了100 000个比特币作为准备金，那么它们会发起一笔100 000个比特币的转账交易，收款人就是交易所本身，然后向客户说明这笔交易的有效性。之后，它们会用同一个私钥去为一条查询指令签名，这个查询指令是公正的第三方随意发出的字符串。这样就可以证明出具准备金证明的人至少知晓该私钥（即使他不是私钥的拥有者）。

我们应注意到两点：首先，严格地说，准备金证明并无法证明交易所真正拥有这些准备金，只能说明真正拥有这笔比特币的人愿意参与准备金证明的过程。换句话说，准备金证明只是证明了某人（交易所）可以控制这一笔钱，或者某人（交易所）所熟悉的人可以控制这一笔钱。其次，准备金是可能被瞒报的，一个交易所可能留存了150 000个比特币的准备金，但只向人们证明它留存了100 000个比特币的准备金。因此，准备金证明不能证明准备金的上限金额，而只能证明其下限金额，即证明某人（交易所）“至少”有多少准备金。

负债证明（proof of liabilities）

目前，交易所只证明了留存的准备金规模，为了证明准备金留存比例，还需要证明其吸收的存款规模。知道了准备金规模和存款规模，那么将这两个数相除就得到了准备金留存比例。我们接下来会展示一种方法，可以确保交易所不会瞒报存款规模（但可以多报），这样，由于交易所向人们证明了准备金“至少”是多少，存款规模“至多”是多少，这样，在计算准备金比例时，分子偏小而分母偏大，因此，我们可以得到准备金比例的保守估计。

对于比特币交易所而言，如果不考虑储户隐私的话，可以将所有的存款记录公布，即公布所有储户的姓名和金额，这样，人们就可以计算交易所的储蓄规模（即交易所的负债规模），而且，如果交易所瞒报数据，那么某些储户将发现自己并不在公布名单内或者发现自己的储蓄额少了，这时，储户就会将此曝光，因此，交易所不可能瞒报存款规模。但是，交易所可以在存款记录中加入一些虚构的客户，这样，由于公布的数据真假掺和，在一定程度上可以保护储户的隐私，只是这么做会使交易所的总负债被高估。这种情况下，只要没有收到储户投诉其储蓄被少报或漏报，人们就可以相信，交易所公布的负债规模肯定不低于实际的负债规模。

当然，以上做法是以牺牲储户隐私为代价的。实际上，我们会用梅克尔树来证明存款规模。我们在第1章就说过，梅克尔树就是一棵哈希值构成的二叉树，每个指针不仅告诉我们去哪里找到一个信息，而且还告诉我们这个信息的哈希值。交易所想要证明其负债，可以先构建一棵二叉树，二叉树的每个叶节点都代表一个储户，如图4.5所示（当然，这里也同样需要储户来核实自己是否在这棵二叉树上），之后，我们还需要让储户可以核实交易所声明的负债规模，要实现这点，我们需要为每个节点添加一个字段（下文简称为存款金额字段），这个字段显示其最近的两个子节点的存款金额之和。

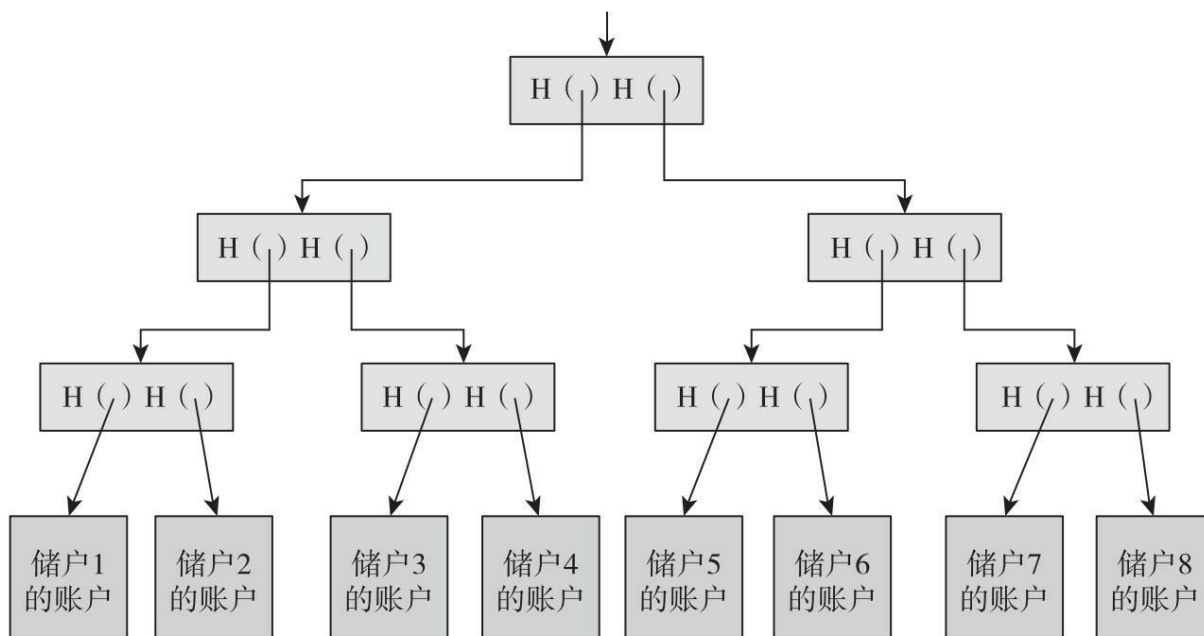


图4.5 负债证明

注：交易所构建这样一棵梅克尔树：每个储户对应一个叶节点，每个叶节点的存款金额字段保存储户存款金额。每个节点的存款金额字段等于与其最相近的两个子节点的存款金额之和，这样，根节点的存款金额字段就代表着存款总规模。每个储户都可以要求交易所证明该储户在梅克尔树上，并且可以核实根节点所显示的总存款规模。

交易所构建完梅克尔树之后，把根节点的哈希指针和根节点的存款金额字段进行加密签名，然后在网络上广播。根节点的存款金额字段自然就是存款总规模——也就是我们最关心的数据。此外，交易所还需要声明所有储户都可以对应到叶节点上，而且所有储户的存款数据都是正确的，并且每个父节点在加总子节点的存款数据时也没有出现差错，因此，根节点的存款金额字段正确无误地说明了存款总规模。

现在，每个客户都可以向交易所索取存款证明，交易所也必须向储户出具相应证明。这种证明实际上就是一棵包含该客户所对应的节点的子树，子树应包括根节点和叶节点，如图4.6所示，之后，客户可以核实以下几点：

- 1.子树根节点的哈希指针和存款金额字段，与交易所广播的值一致。

2.从子树的根节点遍历到叶节点，每个节点对应的哈希值确实是其所指向的子节点的哈希值。

3.每个叶节点对应的客户账号信息（客户名、账号和存款金额）都是正确无误的。

4.每个节点的存款金额字段正好等于与其最相近的子节点的存款金额之和。

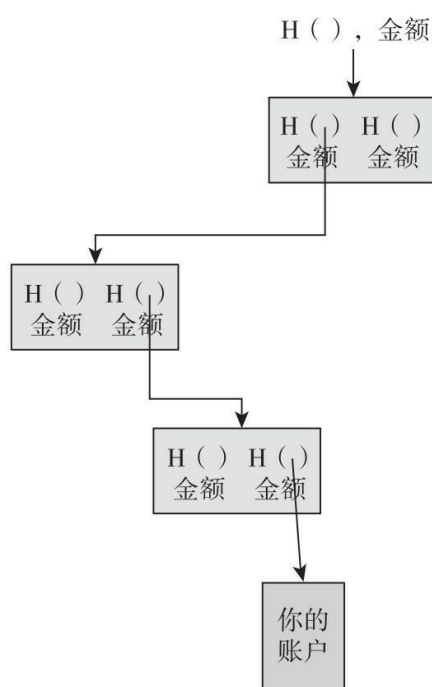


图4.6 以梅克尔树（子树）的形式提供存款证明

注：子树包含叶节点、根节点和之间的所有子节点及其兄弟节点。

上述做法的优点在于，二叉树的每个分支都会被遍历一遍，而且，总有人会核实每个节点的存款金额字段恰恰等于与其相邻的两个子节点的存款金额之和。关键的是，不同的客户获得的子树中，如果有相同的节点，那么这些节点的哈希值以及存款金额字段也必定是相同的，否则就会产生哈希碰撞（hash collision）。

我们总结一下。首先，交易所为了证明其留存了X比特币的准备

金，发起了一笔向自己转账的交易，转账金额为X个比特币，并且在网络上广播这笔交易。之后，交易所证明其吸收的存款规模不少于Y比特币。这样，我们就知道这个交易所的准备金比例至少是X/Y。这意味着，如果一个比特币交易所想向人们证明自己的准备金比例是25%，可以通过上述方法让所有人都可能对此进行独立审计，而不是依靠中央权威机构来验证。

你也许发现了上述两种方法（存款证明和负债证明）泄露了很多私密信息，其中包括很多敏感信息，例如交易所使用的账户、存款准备金总规模以及交易所总负债规模，甚至是储户的个人账户余额等。实际上，交易所并不愿意公布这些信息，因此在实际应用中，存款准备金证明用得很少。

最近推出的一个被称为“准备金”（provision）的协议，也可以提供偿付能力证明，而且不需要披露总负债和总的存款准备金规模，也不需要披露正在使用的账户地址。该协议使用的加密技术更加先进，在此不深入讨论。但是这个技术又一次证明，加密技术能够帮助保护隐私。

偿付能力是一项可以执行的监管措施（比特币交易所可以自主选择遵守），其他方面的监管措施则更难执行，请参见第7章。

4.5 支付服务

到目前为止，我们讨论了如何存储和管理比特币。现在我们来讨论一下商户——无论是电商还是实体店——如何接受比特币付款。通常，商户接受比特币付款只是为了满足客户使用比特币支付的需求，其实商户并不愿意持有比特币，因此他们需要快速地把比特币换成法币。对于商户来说，他们希望这个过程——收款和兑换——可以尽可能简便地实现，最好是不需要了解太多技术细节。例如，不需要对他们现有的网站大动干戈，或重新购置支付设备。

商户还希望整个过程是低风险的。实际上，商户接受比特币付款可能面临多种风险。例如，使用新技术可能使他们的网站崩溃而造成损失；使用比特币还可能存在安全风险，黑客可能攻破商户的在线钱包，或者雇员可能携比特币潜逃；最后，比特币还可能有汇率风险——比特币的汇率随时间波动很大。对一个商户而言，如果他的比萨定价是12美元，那么每卖出一张比萨，商户希望收到的钱是12美元，如果他接受比特币付款，那么他会希望比特币的价格不要出现太大的波动，他要保证所收到的比特币能兑换回来12美元。

支付服务商就在这种背景下发展起来了，可以同时满足客户和商户的需求。

站在商户的角度，客户用比特币支付的整个流程如下：

1. 商户登录支付服务网站，如图4.7所示（图来自比特币基地公司的网站界面，译者翻译），按照网站的要求，填写商品名称、数量、商品描述、收款账户等信息。

选择使用比特币支付，或观看每种支付方法的示例。

类型 ☒ 按钮 ☐ 托管网页 ☐ iFrame ☐ 电邮发票

支付方式 ☒ 现在支付 ☐ 捐赠 ☐ 订阅

按钮类型 ☒ 使用比特币支付  ☐ 使用比特币支付 

☐  使用比特币支付 ☐  使用比特币支付

商品名称 数量

商品描述

支付给
显示更多选项

图4.7 生成比特币支付按钮的软件界面示例

注：通过支付服务商提供的网站，商户可以轻松生成一段网页代码，直接嵌入商户的现有网页即可使用。

2.支付服务商网站会根据商户所填的内容，生产HTML代码，商家可以直接将代码添加到现有网页代码中，这时，网页中就会出现一个支付按钮。

3.客户在商户网站上点击支付按钮，后台就会执行整个流程，最后商户会收到确认信息：“[客户]购买了[数量]的[物品]，支付了[金额]”。

这种手动添加按钮的做法，只适用于只卖一两个物品的小网站，或用于接受捐赠的网站，对于大型的购物网站，手动复制粘贴成千上万次

代码显然是不现实的。因此，支付服务商网站也提供可编程的界面来为动态页面添加支付按钮。

现在，我们来看一看，当客户使用比特币进行网购时，整个付款流程的细节是怎么样的（下面所说的步骤，正是图4.8描述的流程）。

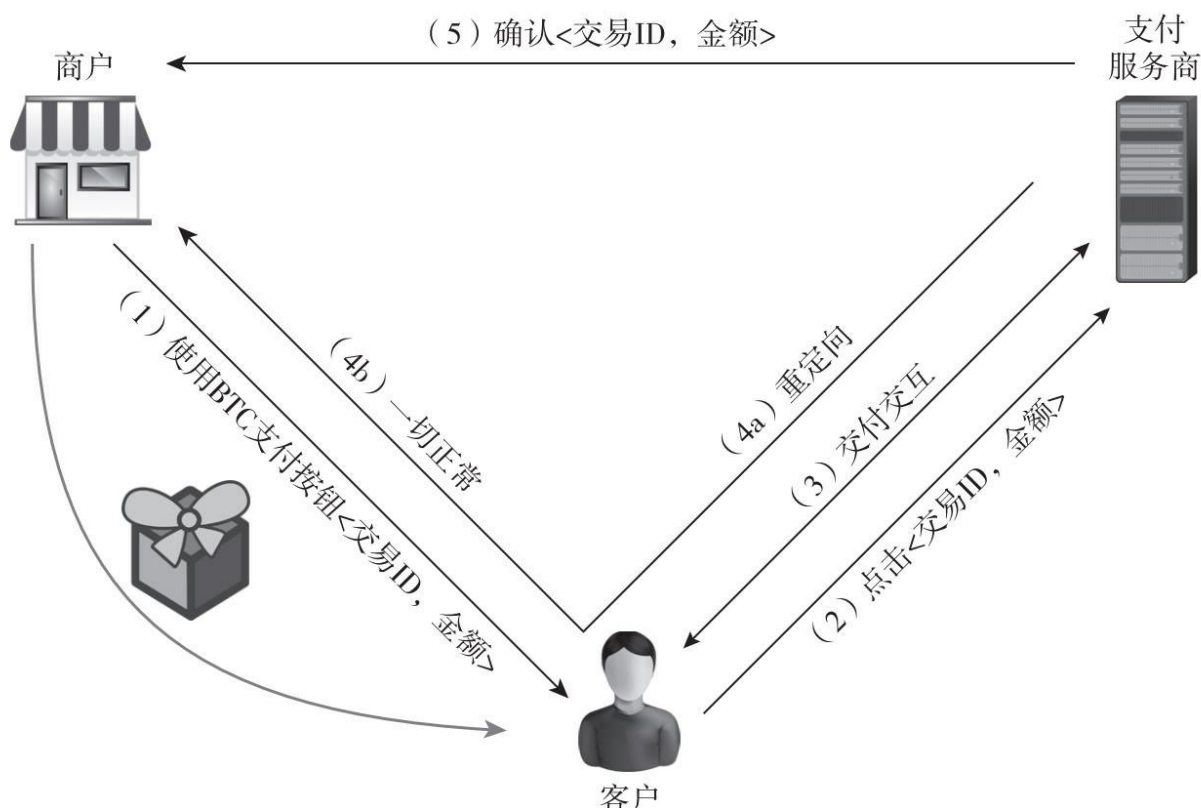


图4.8 客户、商户和支付服务商的交互流程

1.客户在购物网站上挑选了一个商品，当他打算付款的时候，会跳转到一个付款页面，页面上有“用比特币支付”的按钮（通过嵌入支付服务商提供的HTML代码实现），此外，页面上还会显示一个交易ID（便于商户记账）和金额。

2.如果客户想用比特币支付，就会点击对应的支付按钮，这时，网页会向支付服务商发送一个HTTPS请求，告诉支付服务商现在有个客户想用比特币支付，网页还会向支付服务商传送商家ID、交易ID、金额等

数据。

3.支付服务商收到数据之后，知道有客户——无论他是谁——想要支付一定金额的比特币，这时，网页会弹出一个窗口，提示客户付款流程，客户根据提示发起一笔转账申请，从他的钱包中转移一部分比特币给支付服务商。

4.客户付款后，网站会重新跳转到商户页面，并提示付款流程正常。这意味着支付服务商在比特币网络上收到了这笔交易的广播，但这个交易还没有通过足够多节点的核验。从客户角度来讲，他已经完成支付，但从商户的角度讲，还需要等待支付服务商的确认才可发货。

5.最后，支付服务商直接向商家发送付款凭证（交易ID和金额），这表示支付服务商承诺会支付这笔钱给商户，这时商户才开始发货。

整个支付服务的最后一个环节是支付服务商向商户结算并付款——将相应金额的美元或其他货币直接转到商户的银行账号。结款频率可能是每日数次或每日一次，但不会每笔交易都结算一次。支付服务商按比例收取服务费用，这就是支付服务商的盈利模式。不同的支付服务商，上述流程细节可能有所不同，但大抵相似。

简单总结一下，通过支付服务商的服务，客户可以用比特币购物，商户如期收到美元，支付服务商获得手续费，皆大欢喜。对商户来说，他只关心销售物品，收回美元或其他通行的货币，中间的一切环节由支付服务商打理：收取客户的比特币，并兑换成货币给商户。

关键的是，在整个过程中，支付服务商承担了所有风险。首先，它承担了安全风险，所以需要好的安全措施来管理比特币；其次，它承担了汇率风险，它收取比特币然后支付美元，如果美元兑比特币的汇率波动太大，支付服务商可能会遭受损失，但如果汇率往有利的方向波动，

也可能大赚一笔。支付服务商的商业模式决定了它必须承担风险。

需要注意的是，支付服务商的资金流动很大，它收取大量的比特币，然后付出大量的美元。因此，支付服务商自然就成为交易所的活跃成员——通过交易所才能实现法定货币与比特币的通兑。对于支付服务商而言，不仅需要考虑比特币的汇率问题，也要考虑如何进行巨额兑换。当然，如果一个支付服务商解决了这些问题，就可以解决客户想付比特币而商户想收美元的矛盾，为此，支付服务商从每笔交易中收取的手续费有可能使其实现相当可观的利润。

4.6 交易费

前面的章节中已经提到过交易费，以后的章节也会陆续提到。本章主要讨论在比特币系统中，交易费是如何设定的。

当一笔交易被纳入比特币区块链的时候，就可能支付了一笔交易费。前面章节提到，交易费是比特币交易中输入金额（付款方支付的比特币）和输出金额（收款方收取的比特币）之间的差额——输入金额必须不少于输出金额，否则交易无法完成；如果交易的输入金额大于输出金额，那么这个差额就是交易费。交易费由将该交易打包进某个区块的矿工获得。

交易费的经济意义非常有趣，也非常复杂。而且交易费的设定细节随时间变化而不断变化，我们在这里把时间框定在2015年年初，讨论交易费在那个时点是如何设定并运作的。我们也会在本节末尾简单叙述一下当前的情况。

交易费为什么存在？原因是在比特币网络中传播你的交易信息是需要成本的——每个节点传播交易信息，最后由一个矿工把这笔交易打包进一个区块，这些都有代价。举个例子，如果一个矿工将你的交易打包进他的区块，那么这个区块就会比其他区块大一点点，也会花费更多的时间传输到其他节点，这样，这个区块变成孤块的可能性就会提高，原因是在这一小段时间中，别的矿工也许刚好完成了区块打包。

不论是对于节点的传播还是对于矿工而言，确认你的交易都需要花费代价，交易费便用来补偿矿工处理交易所付出的代价。节点通常并不收取费用，当然，节点的运行成本也比矿工的运行成本低许多。交易费的金额可以由发起交易的人自由设定，也可以不设定交易费。通常来讲，如果你支付了较高的交易费，则交易将被更快、更可靠地传播和记

录。

为了说明矿工如何设定交易费用，我们现在来看一下默认的交易费政策。但需要注意：首先，下文叙述的交易费政策基于2015年发布的现行第0.10.0版本，在后续版本中，交易费政策可能不同；其次，设置默认交易费的动机是为了防止区块链被大量小额交易所“污染”，而并不是想准确地评估矿工处理交易的成本。

当然，矿工无须遵守默认的交易费政策。在2015年，交易费在矿工收入中的占比不到1%，因此，大部分矿工是遵循默认交易费政策的。但随着挖矿奖励的降低，交易费在矿工收入中的占比会越来越高，我们可以预测，将会有越来越多的矿工不再遵守默认的交易费政策。

现在大部分矿工所默认的交易费是这样计算的：首先，如果交易满足以下三个条件，那就不需要支付交易费：

- 1.交易小于1 000个字节。
- 2.所有输出为0.01BTC或更大。
- 3.优先权足够高。

优先权是这样定义的： $(\text{所有输入的账龄的总和} \times \text{输入金额}) / \text{交易规模}$ 。也就是说，先明确交易的输入所对应的上一笔交易，把每笔交易的账龄（交易完成到现在所经过的时间）及输入金额相乘，然后把乘积相加，就得到了优先权数据。注意，某笔交易的输出越长时间没有被消费掉，账龄就越高，那么，它被支付时，交易的优先权就越大。

如果一笔交易满足了上述三点要求，这笔交易会被传播，最后会被纳入区块链，这个过程是免费的。否则，交易就会被收取费用，当前默认标准是：每1 000个字节需要支付0.0001BTC，在2015年，这相当于每1 000个字节花费1美分的交易费，一笔交易通常包括：输入通常是148

个字节，每个输出通常是34个字节，其他信息10个字节。如果一笔交易有两个输入和两个输出，那么这笔交易的大小是400个字节。

如果一笔交易没有满足上述要求，它也有可能被纳入区块链，但如果你想要一笔交易被更快、更有保证地纳入区块链，那么就需要支付一笔标准的费用。因此，大部分钱包软件和支付服务商在它们的支付流程中，都包含了标准的交易费用，在日常比特币交易过程中，你会发现你支付了一定的交易费用。

当前，大多数的矿工会强制要求交易必须包含交易费，这意味着他们不会去处理那些没有付交易费的交易（或者最后处理）。当然也有些矿工没有这么做，他们愿意接受很少的交易费用甚至免费。

4.7 货币兑换市场

这里所说的货币兑换市场是用比特币来交易美元或是欧元。虽然前面谈到的支付服务也能做到这一点，但这里讨论的是整个货币兑换市场，包括市场规模、分布、如何运转，以及与这个市场相关的经济学原理。

首先，比特币兑换市场的运作和法币兑换市场的运作很相似。货币兑换价格的涨跌取决于人们买入美元或欧元的需求。在比特币世界里，有不少网站（例如bitcoincharts.com）可以告诉你比特币与不同货币之间的汇率。

在这个网站上，可以看到有很多交易正在进行，汇率也持续在发生波动。比特币市场具有高度的流动性，你可以在很多场所兑换比特币。2015年3月，Bitfinex（最大的比特币和美元兑换交易所）的每日交易量大约是70 000比特币，或是2 100万美元。

当然，人们也通过当面交易的方式兑换比特币。有许多网站提供这种服务，举个例子，在localbitcoins.com，你可以告诉别人你的位置，然后告诉大家想以什么样的价格购买多少比特币，之后，网站会告诉你当地有多少人愿意在约定的地点出售比特币，还会告诉你他们出售比特币的数量和价格。这样，你就可以联系他们，约在一个咖啡馆或公园，或者其他什么地方进行交易——支付美元购买比特币。对于小的交易，在交易完成之后，你们只需等待一小段时间，交易便可以在区块链上被确认。

交易变得越来越频繁，人们开始定期在固定地点碰头，进行比特币交易。例如，你可以在固定的地点，去某个公园、街角或者咖啡店，大家都在那里聚会，进行比特币的买卖交易。有很多人喜欢这样的线下交

易，与交易所在线交易相比，线下交易可以保护用户的个人隐私，而根据银行的监管要求，人们在交易所开户需要提供身份证明，无法实现匿名。我们将在第7章中对此展开讨论。

供给和需求

就像其他市场一样，比特币交易所撮合买家与卖家。交易所是一个相当大的市场，每天的交易量都在数百万美元的规模。当然，它还比不上纽交所或是能和美元/欧元外汇市场相提并论，但它也成了一定的气候，而且比特币兑换也形成了公允市场价格。一个交易员想在交易所买卖比特币，总是可以找到交易对手——至少在交易额不太巨大的情况下如此。

和任何一个其他流动的市场相似，比特币市场中的公允价格是由供给和需求决定的。供给是指比特币的供给，即可能被出售的比特币的数量；需求是指人们对比特币的需求，他们持有美元，想购买比特币。通过市场的供给和需求机制，比特币的价格会被设定为一个价格，在这个价格下，比特币的供给和需求刚好相等。我们稍微讨论一下细节。

比特币的供给是多少呢？供给就是指人们可能买到的比特币数量，也就是整个市场中正在流通的比特币数量，这个数值是固定的，在2015年年末，这个数值是1 500万，根据比特币的设计，比特币数量将缓慢上升，最终达到2 100万的上限。

在考虑比特币供给的时候，也可以将活期存款考虑在内。如果人们在交易所存入比特币，而交易所并没有全额提取准备金，那么实际上，活期存款总量实际上超出了交易所实际留存的比特币数量。

把活期存款算在比特币总供应量里是否正确，取决于我们如何定义总供应量。如果在我们所分析的市场中，活期存款可以被出售，例如，

如果人们可以用比特币存款兑换美元，而且，人们要求提取活期存款时可以要求交易所支付美元，则活期存款应该被记入比特币总供应量。

值得注意的是，通常情况下，当经济学家谈到法定货币的供应量的时候，他们其实也包括了活期存款，而不仅仅计算市场上流通的货币（即流动的纸币和硬币），原因是人们也使用活期存款来购买商品。所以，当我们说一个市场上比特币的供应量固定在1 500万或者最终增加到2 100万时，我们需要把那些可以等同于现金使用的活期存款也考虑进来，因此，比特币的供应量和某些比特币专家所声称的数量可能不同。我们要针对特定的市场情况来讨论比特币的供应量到底是多少。所以，我们后面讨论比特币供应量的时候，实际上都是针对我们所分析的特定市场而言的。

现在我们再来看一看需求。比特币的需求可以分为两类：一类是将比特币作为支付中介，另一类则是投资需求。

第一，我们讨论作为支付中介的比特币。想象一下，爱丽丝想从鲍勃处购买某个商品，而且希望用比特币来支付（假定爱丽丝和鲍勃其实也可以用美元支付，但他们发现用比特币支付更方便）。我们再假定爱丽丝和鲍勃都不想长期持有比特币，所以，爱丽丝首先会用美元兑换一些比特币用于支付，鲍勃收到比特币之后，会再将比特币兑换成美元。这个例子的关键在于，用于支付的这部分比特币实际上短暂地退出了比特币流通体系。这就产生了比特币的需求。

第二个需求是投资需求。有人想购买比特币并长期持有，等价格上涨之后卖掉。当人们购买比特币并长期持有时，这些比特币也就不再流通。当比特币价格很低的时候，大家都会想买进比特币用来投资；而当价格很高的时候，需求则不会很高。

一个简单的市场行为模型

我们现在做一个简单的经济学建模来理解这些市场行为。我们不会推演整个模型（尽管推演过程很有意思），而是将着重讨论比特币兑换需求对比特币价格的影响。

我们先假设一些参数。 T 是指市场中所有参与者用比特币进行支付的总交易量，该数值用每秒钟发生的交易量（美元）来计量，我们假定人们在进行支付的时候，也总是想着比特币的美元价值，这样会简化问题。这样，我们就可以用美元来衡量每秒钟的总交易量。 D 是指比特币用于支付时，暂时退出流通体系的这段时间长度——从付款者买入比特币开始到收款人将比特币兑换回市场为止，以秒计算。 S 是人们可以买到的比特币总量，等于比特币总量——目前是1 500万左右（未来会增加到2 100万左右）——减去人们打算长期持有的比特币数量，也就是在市场上流通的、可以随时买卖的比特币总量。最后， P 是比特币对美元的价格。

现在我们可以做一些计算。首先，我们要计算一下每秒钟有多少比特币可以被用来做交易。在 D 秒内，市面上有 S 个比特可以用于交易，所以每秒钟有 S/D 的比特币重新进入流通体系，可以用于支付。这是供应侧的数据。

在需求侧（指每秒钟所需的用于支付交易的比特币数量），我们总共的支付交易规模是 T 美元，而每1美元对应的交易，我们需要 $1/P$ 个比特币来完成。所以， T/P 就是我们每秒钟所需的用于支付交易的比特币数量。

在特定的某秒钟内，供应是 S/D ，需求是 T/P 。和其他市场一样，价格会根据供需关系达到平衡。如果供应大于需求，有些比特币就卖不出去，出售的一方不得不降价出售。同样地，根据我们 T/P 的需求公式，当价格下降后，需求增加，供应与需求会再次达到平衡。

另一个方面，如果供应小于需求，这意味着有些人想购买比特币用

于支付，但是买不到，这些人就必须出更高的价格来购买，而当价格升高后，需求就会下降，供应与需求也会再次达到平衡。所以我们可以得到以下公式：

$$S/D=T/P$$

从中我们可以推算出价格的公式：

$$P = \frac{TD}{S}$$

这个公式说明什么？我们可以将其更加简化：我们假设D（也就是比特币用于支付时，暂时退出流通体系的这段时间长度）不变，人们可以买到的比特币总量S也不变，或至少变化的速度很缓慢。这意味着价格P和需求T是成正比的。所以，如果需求翻倍，比特币价格也会翻倍。我们可以根据比特币的实际价格以及我们估计的需求量做图，看看价格和需求的关系是否真的和我们所预测的一样。经济学家们已经证实了这一关系。

请注意，S（人们可以买到的比特币总量）并不包含那些用于投资而被长期持有的比特币。所以如果越来越多人购买比特币用于长期投资，则S会下降，根据上面的公式，P会上涨。这很容易理解，当持有比特币作为长期投资的人增多，用于支付中介的比特币的价格自然上涨。

这并不是一个完整的市场模型。一个真正的市场模型还必须考虑投资者的心理活动，如果投资者相信比特币价格会上涨，他们对比特币的需求就升高。这就是我们所说的投资者预期，加入投资者预期后，模型会变得很复杂，我们在这里不展开讨论。

总之，存在比特币和美元、比特币和其他货币的兑换市场。这些市场有足够的流动性，你可以兑换或买卖比特币，这种兑换很可靠，当然

价钱会有波动。我们可以用经济学模型来理解供给和需求对市场的影响，如果我们有办法估计一些不可知的信息，比如说未来人们需要多少比特币用于支付，我们就可以预测市场。经济学模型很重要也很有用，现在也有很多人从事更细节的研究，但详细的经济学模型并不在本书的讨论范围。

延伸阅读

比特币的安全机制和银行的安全机制类似，但也有些重要的差异。Ross Anderson的安全机制教材一书中的第10章“Banking and bookkeeping”，非常值得一读，教材可以在网络上免费获得：

Anderson,Ross. Security Engineering .Hoboken,NJ:John Wiley & Sons,2008.

分析比特币交易所为何倒闭的书籍，建议阅读：

Moore,Tyler,and Nicolas Christin.“Beware the Middleman:Empirical Analysis of Bitcoin-Exchange Risk.”In Financial Cryptography and Data Security. Heidelberg:Springer 2013.

Adi Shamir关于密码分存的书籍：

Shamir,Adi.“How to Share a Secret .”Communications of the ACM 22（11），1979.

讨论Provisions（无须泄露储户隐私的偿付能力证明协议）的相关书籍：

Dagher,Gaby and Benedikt Bünz, Joseph Bonneau, Jeremy Clark, and Dan Boneh.“Provisions:Privacy-Preserving Proofs of Solvency for

Bitcoin Exchanges.” In Proceedings of the ACM Conference on Computer and Communications Security .New York:ACM Press,2015.

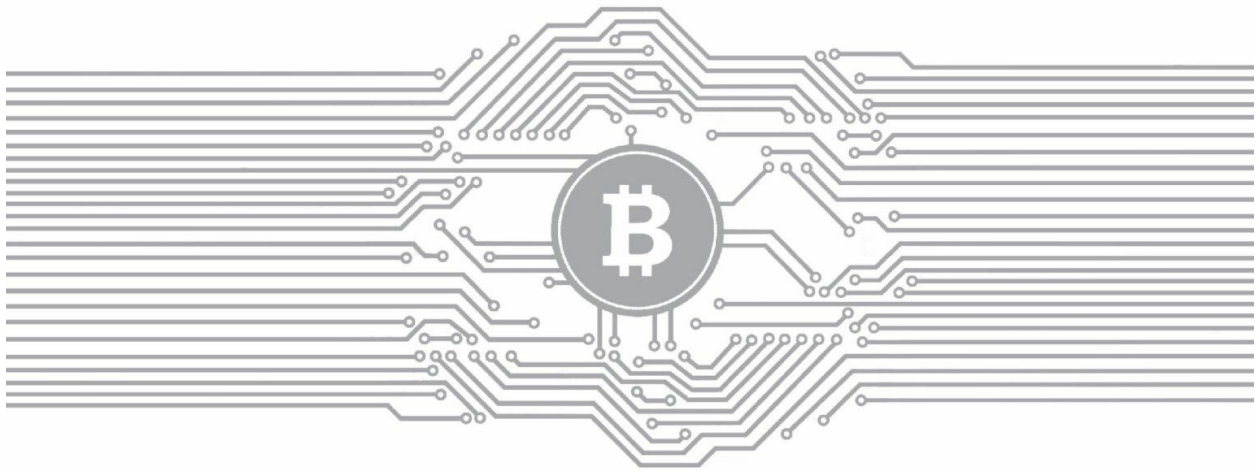
一个密码很难又好记又安全——现在的密码破解技术越来越巧妙、有效，下面的文章有相关示例：

Weir,Matt,Sudhir Aggarwal,Breno De Medeiros,and Bill Glodek.“Password Cracking Using Probabilistic Context-Free Grammars.Presented at the 2009 IEEE Symposium on Security and Privacy,Oakland,CA,2009.

关于2014年比特币交易费的调查报告：

Möser,Malte and Rainer Böhme.“Trends,Tips,Tolls:A Longitudinal Study of Bitcoin Transaction Fees.”Presented at the Second Workshop on Bitcoin Research, Puerto Rico, 2015.

第5章 比特币挖矿



这一章节我们将着重讨论比特币挖矿（bitcoin mining）。前面我们已经讨论了比特币是如何依赖这些矿工们而运行的——他们查证交易记录，制造和储存所有的区块，并对被写入区块链的区块达成共识。我们还知道矿工们会从中得到一些奖励，但还是有些悬而未决的问题：这些矿工都是谁？他们是如何进入这个行业的？他们是怎么运作的？他们的商业模式是什么？他们对环境造成什么影响？我们将在这一章节回答这些问题。

5.1 比特币矿工的任务

你若是想加入比特币挖矿行列，我们不会极力劝阻你，但会提醒你比特币挖矿潮很像当年的淘金热。历史上的淘金热充斥着各种年轻的淘金者下海淘金发财的故事，并且不可避免地，许多人最终失去了一切。在这些确实经历了千辛万苦的人们当中，也只有少数人变得富有。我们将在本章中了解到，和传统淘金以及其他快速致富途径一样，比特币挖矿也面临着类似的挑战和风险。我们首先要看一下技术细节。要成为比特币矿工，你必须加入比特币网络并与其他节点相联。建立链接之后，还有六个任务要完成：

- 1.监听交易广播。监听网络上的交易广播，然后验证它们的签名是正当有效的，交易输出没有被重复支付。

- 2.维护区块链网络和监听新的区块。必须先维护区块链。为了做到这一点，一开始你可以要求其他节点把区块链上的历史记录（在你加入区块链网络之前的）同步过来。然后，监听那些被广播到网络上的新的区块。你的任务是验证你收到的每个区块，这里的验证是指保证区块里的每笔交易都是有效的，而且这个区块包含了一个有效的随机数。我们本章后面谈到验证随机数的技术细节。

- 3.组装一个备选区块。一旦拥有最新的全部区块链数据备份，你就可以开始制造你自己的区块了。要做到这一点，你要把所监听到的交易进行组合并放进一个新的区块，然后把该新区块排在整条链中最新的区块的后面。你必须保证你建立的新区块里的每笔交易都是正当有效的。

- 4.找到一个让你的区块有效的随机数。这一步的工作量最大，也是矿工工作中最难的一个环节。我们后面会谈细节。

5.希望你的区块被全网接受。即使你找到了一个区块，也不能保证该区块会成为共识链（`consensus chain`）的一部分。这需要有点运气，希望其他的矿工接受你的区块，然后从该区块开始继续接龙下去，而不是从你的竞争对手发现的区块开始。[\[1\]](#)

6.利润。如果所有其他矿工接受了你的区块，那你就能获取利润。在2015年，一个区块的奖励是25个比特币，大约在10 000美元左右。此外，如果在该区块里的任何交易都有交易费，所有交易费也会为矿工所有。到目前为止，交易费作为额外收入，相对来说还比较低，大概是一个区块默认奖励的1%。

我们可以把矿工的任务分成两类：第一类任务是验证交易和区块，这是比特币网络赖以生存和运转的基础。这些任务也是比特币协议需要矿工的首要原因。第二类任务是和其他矿工竞争，争取可以找到区块并因此获益。这些任务并不是比特币网络存在所必需的，而是为了鼓励矿工去完成第一类任务而设置的。当然，这两类任务都是使比特币成为一个数字货币的必要条件，因为矿工必须获得奖励才会去完成这些重要的任务。

寻找有效区块

现在回到如何找到一个使区块有效的随机数的问题上。在第3章中我们讨论过，区块链主要有两层基于哈希函数的结构。第一层是在区块链上，每个区块的头部都有一个指针指向其前一个区块，第二层是在每一个区块里，包括所有交易的梅克尔树。

作为矿工，首先需要从你的交易池中选出一系列有效的交易并且编译成梅克尔树。当然，只要不超过每个区块随机数的交易上限，你可以选择编译的交易数量。然后，组装出一个新的区块，让它的头部指向区

块链上的前一个区块。新区块的头部，有一个32位的随机数区域。你需要尝试不同的临时随机数，直到该随机数能使整个区块的哈希值小于目标值。这个目标值一般体现为以零开始的特定位数的数值。作为一名矿工，你可能使随机数从0开始，每次增加数值1，直到该随机数能使区块有效为止，如图5.1所示。

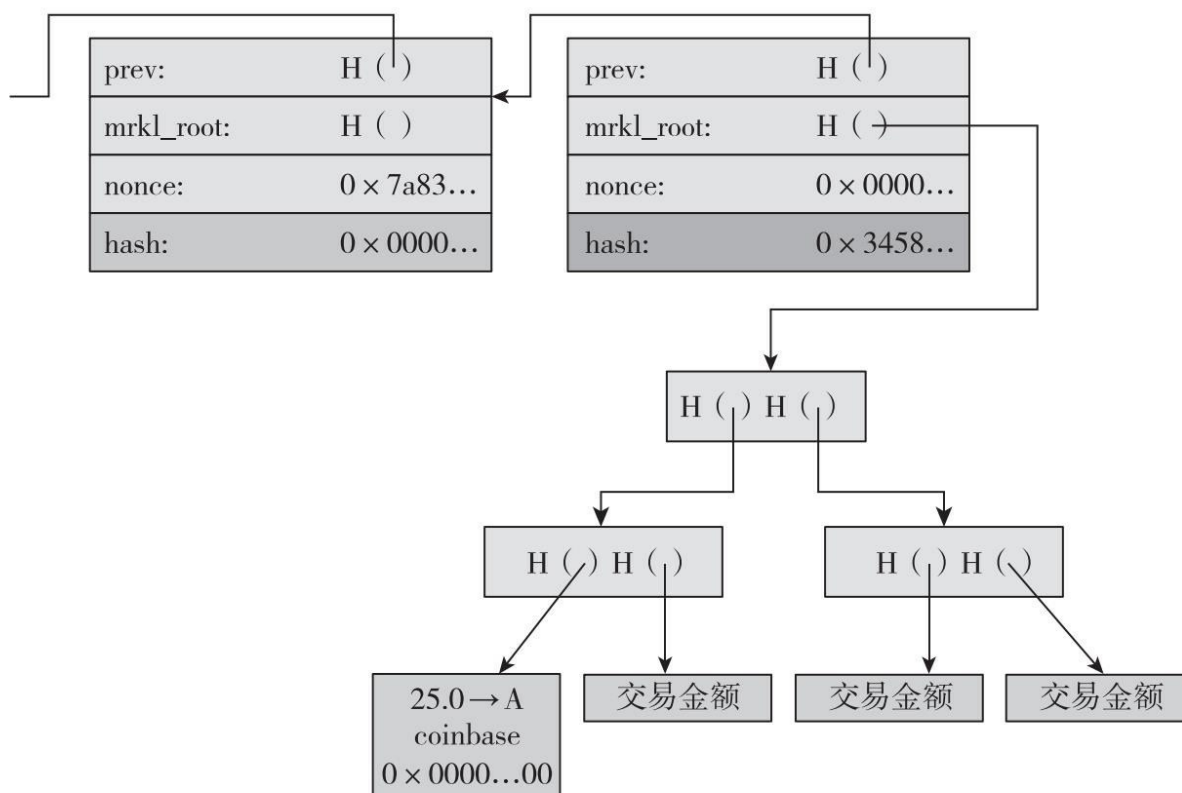


图5.1 寻找有效区块

注：在这个例子中，矿工尝试了一串都是零的临时随机数，但没有产生有效的哈希值，所以矿工继续尝试其他不同的临时随机数。

在大多数情况下，随机数试过所有32位可能的取值后，仍然不能产生一个有效的哈希值，这时候你必须做出更多的改变。注意，图5.1中币基（coinbase）还有一个随机数可以改动。当你遍历区块头部随机数所有可能的取值后，可以改变币基里的随机数，比如加1，然后可以重新改变区块头部随机数来寻找有效的哈希值。

当改变币基里的随机数后，整个梅克尔树上交易的哈希值都会改变（见图5.2），因为币基值的改变会向上传递，所以改变币基的随机数值比改变头部随机数值的代价要大很多。正因为如此，矿工大部分时间只改动头部的随机数，只有在遍历头部 2^{32} 个随机数值且还没有找到一个有效区块时，才改动币基的随机数。

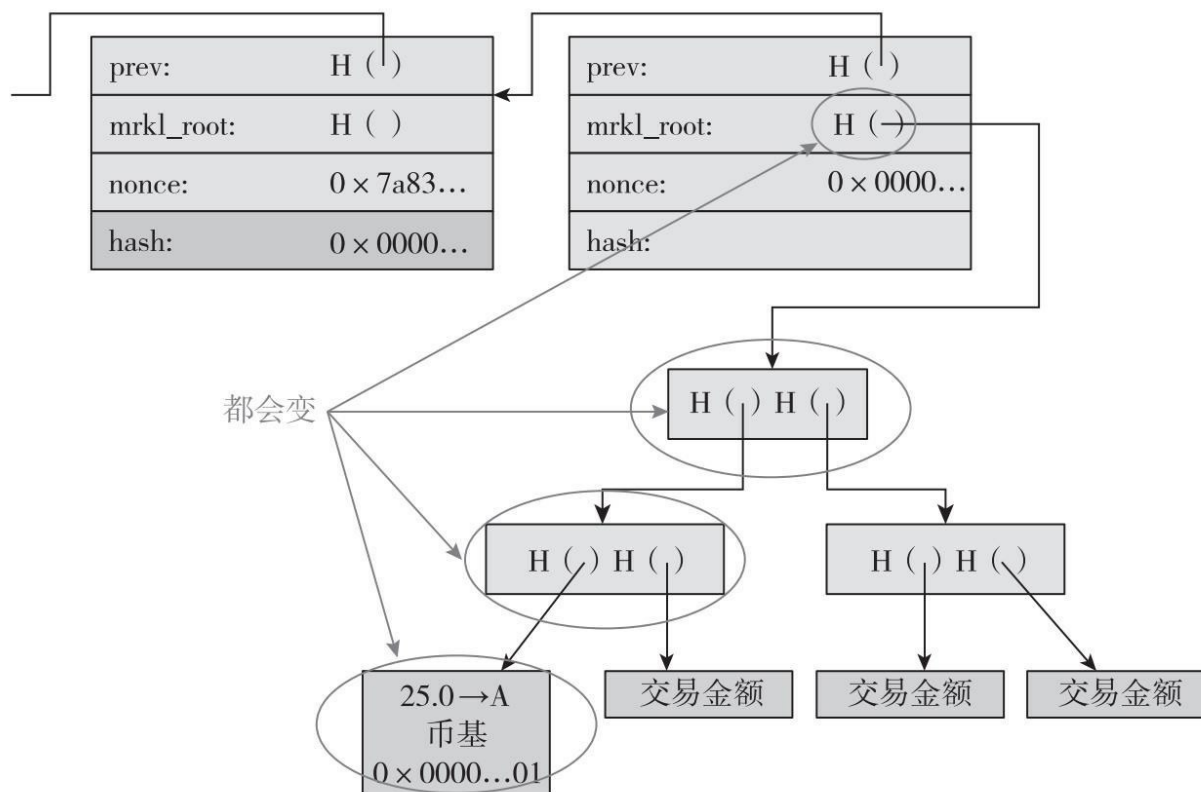


图5.2 改变临时随机数

注：改变币基里的临时随机数，整个梅克尔树的哈希值都会因此而改变。

你所尝试的绝大多数临时随机数都不会成功，但若能够坚持足够长的时间，你总能找到一对正确的临时随机数组合——头部随机数与币基随机数，用来产生一个符合哈希值要求的新区块。找到后要立即宣布，就有希望得到相应的区块奖励。



每个人都在运算同一个谜题吗？

你可能会想，如果每个矿工都在临时随机数值上逐步加1，岂不是大家都在按照同一个运算模式解同样的谜？岂不是最快的一个总赢得竞争吗？不会的。首先，矿工们不太可能在完全相同的一个区块上进行运算，因为每个矿工都会把或多或少不同的交易用不同的次序来放进区块内。但更关键的是，就算两个不同的矿工所组建的区块里包括了一模一样的交易，这两个区块的哈希值还是会不同。请记住在币基交易里，矿工会写自己的地址接收新铸币。这个地址本身的区别会沿着梅克尔树往上传递直达树根，导致整棵树上的哈希函数值不同，从而保证了没有两个矿工的区块是一样的。除非两个矿工共享公开密钥。这种情况只有可能两个矿工同在一个矿池（我们以后会讨论）。同在一个矿池的矿工会互相通信，确保使用不同的币基临时随机数以避免重复工作。

找到一个有效区块到底有多难？到2015年年底，这个挖矿的难度目标区域值（用16进制来表示）为：

00000000000000000172EC000

所以任何有效区块的哈希值必须低于这个值。换句话说，大约 2^{68} 个临时随机数里只有不到一个可以成功，这是一个非常巨大的数值。一个粗略的估计，它比全球人口总和的平方还要大。也就是说，如果地球上的每个人都是一个包含7亿人口的独立星球，那么总人口将会是 2^{65} 。

决定难度

每挖出2 016个区块，挖矿难度会改变一次，这个周期大约是两个星期。难度的改变是根据上2 016个区块的挖矿效率来决定的。用下列公式来表达：

$$\text{下一个难度} = \frac{\text{上一个难度} \times 2\,016 \times 10 \text{ 分钟}}{\text{产生上 2\,016 个区块所花费的时间}}$$

注意，2 016× 10分钟就是两周，也就是说，如果产生一个区块需要10分钟，那么产生2 016个区块就需要两周时间。所以这个公式的意义就是，测量全网难度进而维持平均每10分钟产生一个新的区块的速度。挖矿难度改变的周期是两周，并没有什么特别的意义，只不过是一个权衡之下的结果。如果这个周期太短，难度会随着每一个周期找到的区块的数目的不同而波动（概率问题）。如果太长，整个网络的哈希算力会与难度大大地失去平衡（难度的调整滞后于计算能力的变化）。

每个比特币矿工独立地计算难度，只接受达到这个难度的区块。两个在不同分叉上的矿工可能会有不同的计算难度，但在同一个区块工作的矿工一定会对计算难度达成共识。

图5.3中显示，挖矿难度会随着时间不断地增加。其增加不一定是稳定线性或者是指数型，而是取决于市场行为。挖矿难度会受到有多少新矿工加入的影响，新矿工的加入本身又由比特币的当前价格来决定。总的来说，当越来越多的矿工加入并且挖矿的硬件设备效率越来越高，找到有效区块所花费的时间就会越短，紧接着难度就会增加，直到重新回到每10分钟找到下一个有效区块。

在图5.3中，虽然整个网络的哈希速度是平滑向上增长的，那条实线代表的难度却呈现阶梯函数式增长。这是因为每产生2 016个区块才会调整计算难度。

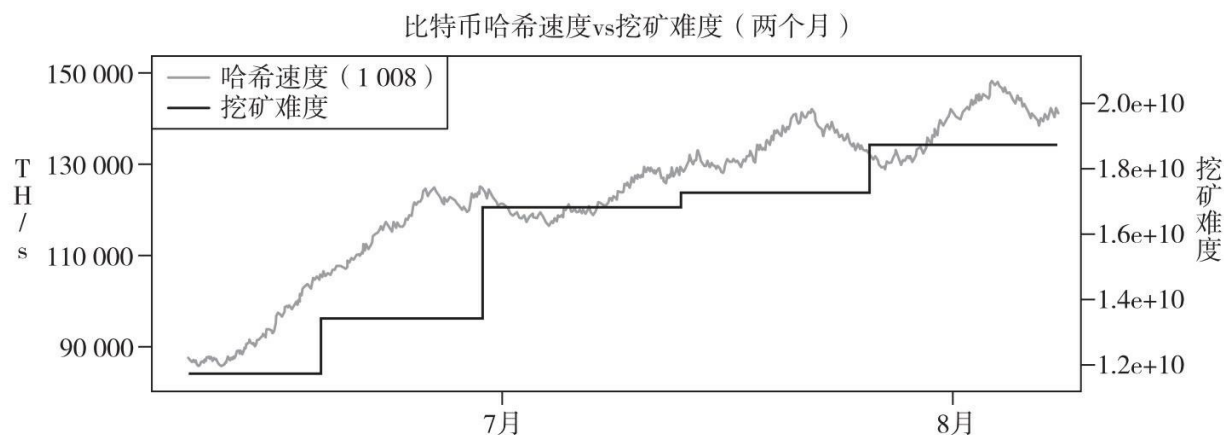


图5.3 挖矿难度随时间变化（2014年年中）

注：y轴开始于80 000TH/s（全网算力）。哈希速度是基于超过1 008个区块计算出来的平均值。

资料来源：bitcoinwisdom.com

可以从另外一个角度来看网络增长率，即看平均要多长时间才能找到一个有效区块。图5.4（a）展示出区块链上两个连续区块产生的间隔时间是多少秒。它逐渐下降，跳升，又逐渐下降。当然产生这种现象的原因就是每2 016个区块之后，难度重新被设定，找到区块的时间又重新回到大约10分钟。虽然一个调整周期内难度都不会变，但是随着越来越多的矿工加入，全网哈希算力增加而难度不变，找到有效区块的速度越来越快，直到大概两个星期内2 016个区块被发现之后，难度会被重新调整。

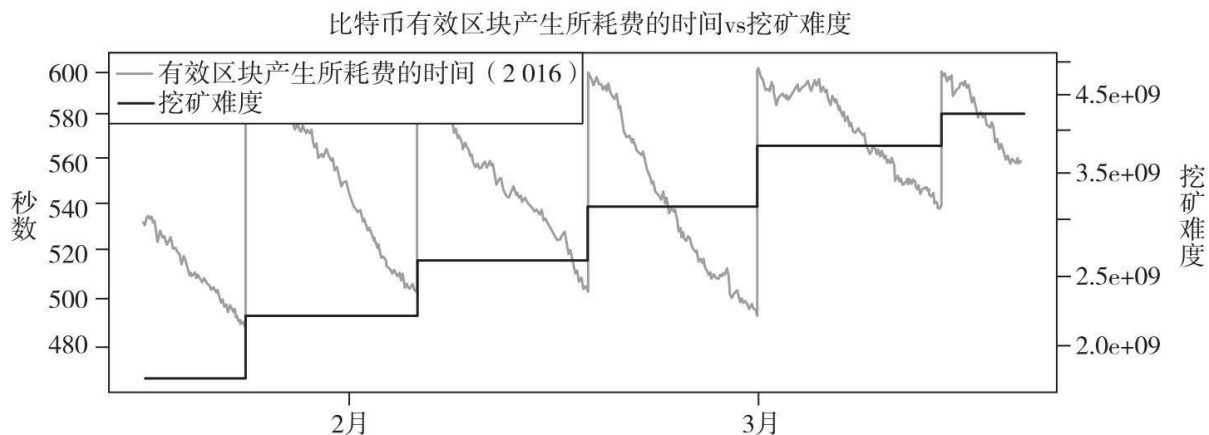


图5.4（a）找到一个有效区块所花费的时间（2014年早期）

注：y轴开始于460秒。找到一个有效区块花费的时间是2 016个区块样本花费时间的平均值。由于当时全网挖矿速度的连续快速增长，找到一个有效区块所花费的时间在两周的时间内稳步减少。

资料来源：bitcoinwisdom.com

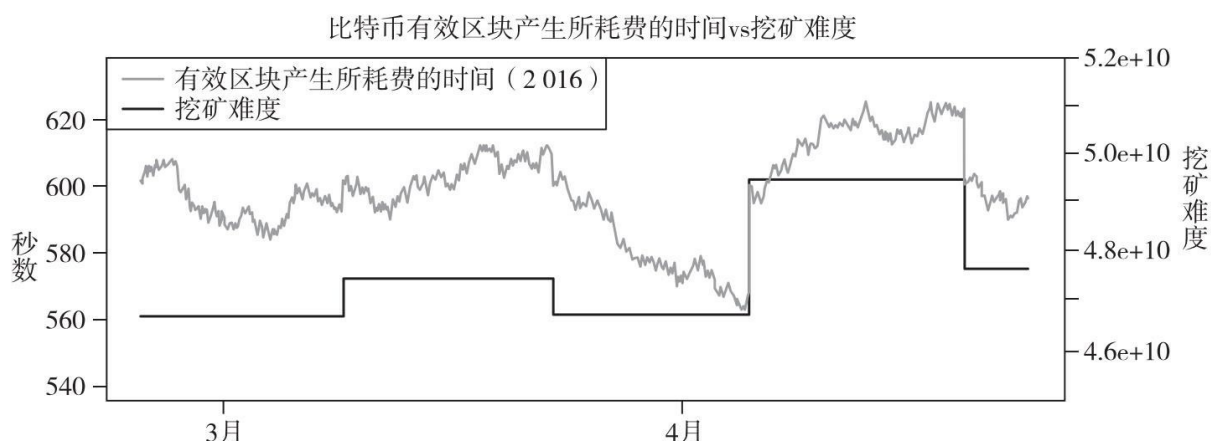


图5.4 (b) 找到一个有效区块所花费的时间（2015年早期）

注：y轴开始于540秒。找到一个有效区块花费的时间是2 016个区块样本建造时间的平均值。由于整个网络增长开始减速，所以找到有效区块的平均时间非常接近10分钟，偶尔还会因为全网算力缩小而超过10分钟。

资料来源：bitcoinwisdom.com

即使找到有效区块的时间目标被设定为平均10分钟，但是在2013年和2014年的大多数时间，这个时间平均是9分钟左右，并且在两周的周期末尾阶段时接近8分钟。计算表明，全网运算能力的增速大概是每两周25%，或者每年几百倍，这个数字非常惊人。

不出所料，这种增长不会无休止地进行，2015年的增速就降低很多（偶尔也会负增长）。在图5.4 (b) 中，我们可以看到全网哈希算力达到了一个稳定的状态，发现每个区块的时间非常接近10分钟，甚至有时会超过10分钟，在这种情况下难度将会被调低。这种曾经被认为不可想象的状况却在2015年频繁发生。

虽然到目前为止，全网哈希算力还没有经历过灾难性的倒退，但是并不排除它发生的可能性。一个有关比特币崩盘的设想被称作“死亡螺旋”，不断下降的比特币价格导致挖矿无利可图，矿工们因此而退出挖

矿（全网运算能力下降），继而进一步导致价格下跌。

[\[1\]](#) 如果下一个区块始于其他人发现的有效区块，你发现的这个区块就会变成无效区块而被丢弃。——译者注

5.2 挖矿所需硬件

前面我们谈到矿工所要做的计算是十分困难的。我们现在谈一下为什么计算如此困难，以及看一看矿工用来进行这些计算所用到的硬件设备。

矿工计算难度的核心在于，对SHA-256哈希函数的运算。我们在第1章抽象地讨论过哈希函数。SHA-256是一个通用的密码学哈希函数，它是在2001年被标准化的密码学哈希函数大家族里的一员。SHA是安全哈希算法（Secure Hash Algorithm）的简称。SHA-256是一个不错的选择，因为它是比特币被发明时可用的密码学哈希函数中保密性最强的。虽然它的安全性有可能随着时间推移而慢慢降低，但至少现在它还是很安全的。SHA-256的设计来自美国国家安全局（NSA），这也导致了一些阴谋论的诞生，但是并不影响它是一个很强的哈希函数的事实。

近距离了解SHA-256

图5.5展示了SHA-256运算的具体细节，虽然我们不需要知道比特币工作原理的所有细节，但是对矿工计算任务的大概了解是很有帮助的。



SHA家族

SHA-256名称中的“256”代表它有256位的状态和输出，技术上来说，SHA-256是SHA-2函数家族中几个密切相关的函数成员之一，包括SHA-512（它有更大的状态位，所以也更加安全）。还有

一个是SHA-1，这是一个有160位输出的早期函数，虽然目前认为安全性不高，但是同样应该在比特币脚本里。

整个SHA-2家族，包括SHA-256在密码学上的安全性是得到公认的，而下一代产品SHA-3家族已经从一个公开的竞赛（由美国国家标准与技术研究所举办）中诞生了。SHA-3目前正在进行最后阶段的标准化测试，但在比特币出现的时候，它还没有出世。

SHA-256是一个256位的状态机。这256个状态被分割成8个32位的字段，这样它可以最优化地运行在32位的硬件上。每一轮运算选择一定数量的字段——有些会进行一些小的逐位调整——最终进行32位模加法运算(modular addition)，然后运算结果被移到状态最左的第一个字段，这样使得整个状态进行向右位移。这种设计的思路来自简单位的线性反馈移位寄存器(Linear Feedback Shift Registers，简称LFSR)。

图5.5展示了一轮SHA-256的压缩函数运算，一个完整的SHA-256运算要做64次这样的迭代运算，在每一轮运算中，会使用稍微不同的常数，所以所有的迭代运算都是不一样的。

矿工的任务就是尽可能快地进行这种函数运算。矿工们互相比拼运算速度，算得越快收益越高。为了实现尽可能快的速度，矿工需要进行32位字段操控，32位模加法运算，同时做按位逻辑运算。

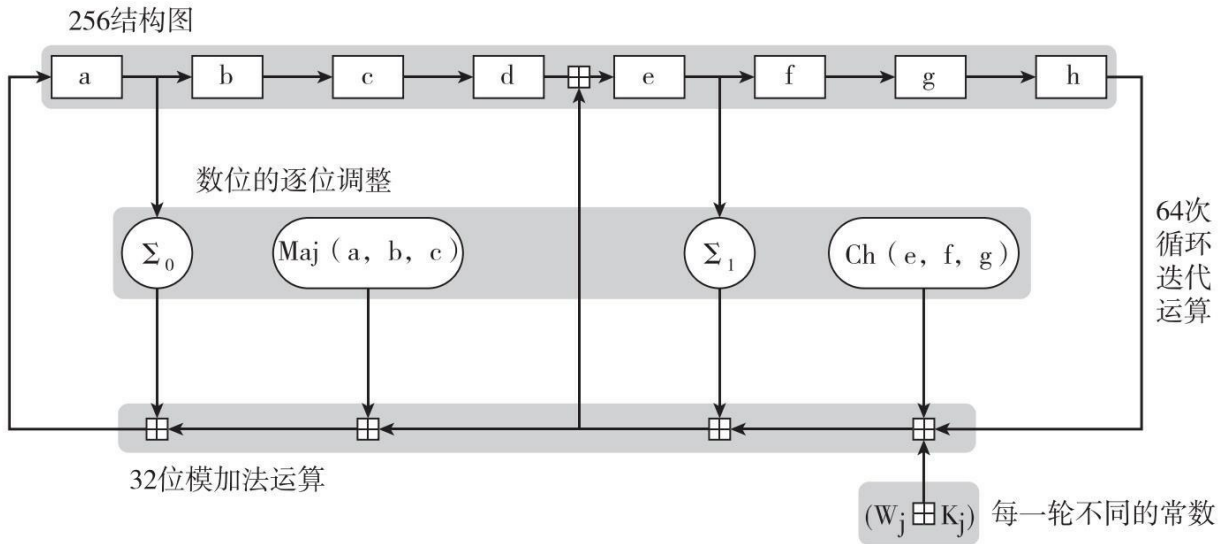


图5.5 SHA-256的结构

注：这是一轮压缩运算。 Maj 是按位运算的。 Ch 也是按位运算的，根据第一个输入值的不同而决定是选择第二个还是第三个。 Σ_0 和 Σ_1 通过按位循环和 \oplus 运算来操纵32位的字符输入。

我们很快就会看到，在比特币机制下，为了得到供其他节点使用的哈希函数，实际上要求两轮SHA-256运算。这是比特币的奇怪之处，进行两次运算的原因并不清楚，但这就是比特币的个性，作为比特币矿工只能服从。

CPU挖矿

第一代挖矿工作都是在普通电脑上完成的，也就是用通用中央处理器（CPU）来进行运算。事实上，CPU挖矿的工作就像图5.6中代码所示的逻辑那样简单，也就是说，矿工简单地按照线性的方式尝试所有的临时随机数，在软件中进行SHA-256的运算，并检查结果确认是否找到一个有效区块。请注意，正如我们之前提到过的，这段代码要进行两次SHA-256运算。


```

TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
    header = makeBlockHeader(transactions, coinbase_nonce);
    for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
        if (SHA256(SHA256(makeBlock(header, header_nonce))) < TARGET)
            break; //block found!
    }
    coinbase_nonce++;
}

```

图5.6 CPU挖矿的伪代码

普通电脑运行这段代码到底有多快？一台高端的个人桌面电脑，每秒可以计算大约2千万次哈希函数（20MH/s），按照这个速度，根据2015年早期的难度水平（ 2^{67} ），大概需要几十万年来找到一个有效区块。毫不夸张地说，挖矿真的非常困难！

如今使用一个普通电脑用CPU挖比特币，在目前的难度下已经无利可图了。在过去的几年里，用CPU挖矿的矿工可能会非常失望地发现，他们永远不可能通过挖矿赚到钱，因为他们不了解比特币是如何运行的。

GPU挖矿

第二代矿工意识到用CPU挖矿是在做无用功，他们开始用显卡或者图形处理器（GPU）来挖。

几乎每一个现代个人电脑都有内置的GPU以支持高性能图像处理，这些GPU都有高吞吐量和高并行处理功能，这两点对比特币挖矿都非常有利，比特币挖矿存在大量的并行处理，因为你需要同步用不同的临时随机数计算多个哈希值。2010年，有一门计算机语言开放运算语言（Open Computing Language，简称OpenCL）诞生了，这是一个可以使

GPU进行非图像处理类工作的通用语言。OpenCL是一门高级语言，人们可以用它在显卡上做很多种类型的运算，而且速度比在CPU上的要快。这给通过GPU来进行比特币挖矿铺平了道路。

当时，通过显卡来挖矿有好几个吸引人的地方。首先，买显卡很容易，而且哪怕是业余爱好者也能轻松配置显卡。你可以在网上或大多数专营电子产品的商场里买到它。对大众来说，显卡是最容易获得的高端硬件设备。其次，显卡还有一些格外适合比特币挖矿的特性：显卡的并行性设计使其具备很多算术逻辑单元（Arithmetic Logic Units，简称ALU），可以同时进行SHA-256运算。有一些GPU还特别集成了针对位移操作的指令，这对SHA-256的运算非常有用。

大多数显卡都可以超频，这意味着如果你愿意承担显卡过热或者出现故障的风险的话，你可以让显卡以高于设计频率的频率更快地运行。超频是游戏玩家们渴望了多年的特性。对于比特币挖矿来说，超频会增加收益，即使超频可能引起一些运算错误。

举例来说，将显卡超频50%，也就是说运算速度加快50%，同时可能会造成SHA-256运算出错概率增加30%。如果显卡错误地接受了一个不正确的运算结果——虽然不太可能发生——你还可以通过CPU来进行二次确认。然而，你可能永远都不会知道一个正确的运算结果被错过了。但是通过超频产生的运算速度的增加，完全可以抵消由于显卡运行错误产生的正确输出减少，这样超频还是合算的（从经济效益上来说）。在上述的例子中，超频使得吞吐量增加到原来的1.5倍，而运算成功率降低到了0.7，那么乘积就是1.05，也就意味着超频使得你的获利增加了5%。为了最大化收益，人们花了很多时间去优化最佳的超频比例。

最后，你可以通过一个CPU和一个主板加载许多个GPU。然后你便可以在安装了多个GPU的电脑上运行比特币节点，监听网络收集交易，组装区块，同时用多个GPU进行SHA-256的运算，以更快地找到正确的

临时随机数及其对应的有效区块。很多人创造性地发明了很多有趣的“自制型”硬件设置，如图5.7所示，用一个CPU来驱动很多个GPU。这种情况仅发生在比特币的早期，当时大多数矿工都是比特币的爱好者，他们并不具备服务器搭建及运营经验。但是他们还是做了很多巧妙的设计，使得大量的GPU可以在一个较小的空间里同时运行，同时还解决了散热的问题。

GPU挖矿的缺点

GPU挖矿也有缺点。GPU有大量的内置硬件来进行图形处理，这些特定硬件对比特币挖矿没有任何用处，比如它们大量的浮点运算单元（floating point units），在SHA-256的运算中完全用不到。



矿工和游戏玩家的对比

根据民间传说，2011年，由于比特币矿工采购了太多的显卡以至于影响到了正常的市场需求，这造成了比特币社区和游戏社区之间的摩擦，因为游戏玩家们发现采购某个热门显卡变得越来越难。有趣的是，尽管如此，很多失望的游戏玩家因此而对比特币产生了兴趣，甚至有些游戏玩家因此而变成了比特币矿工！

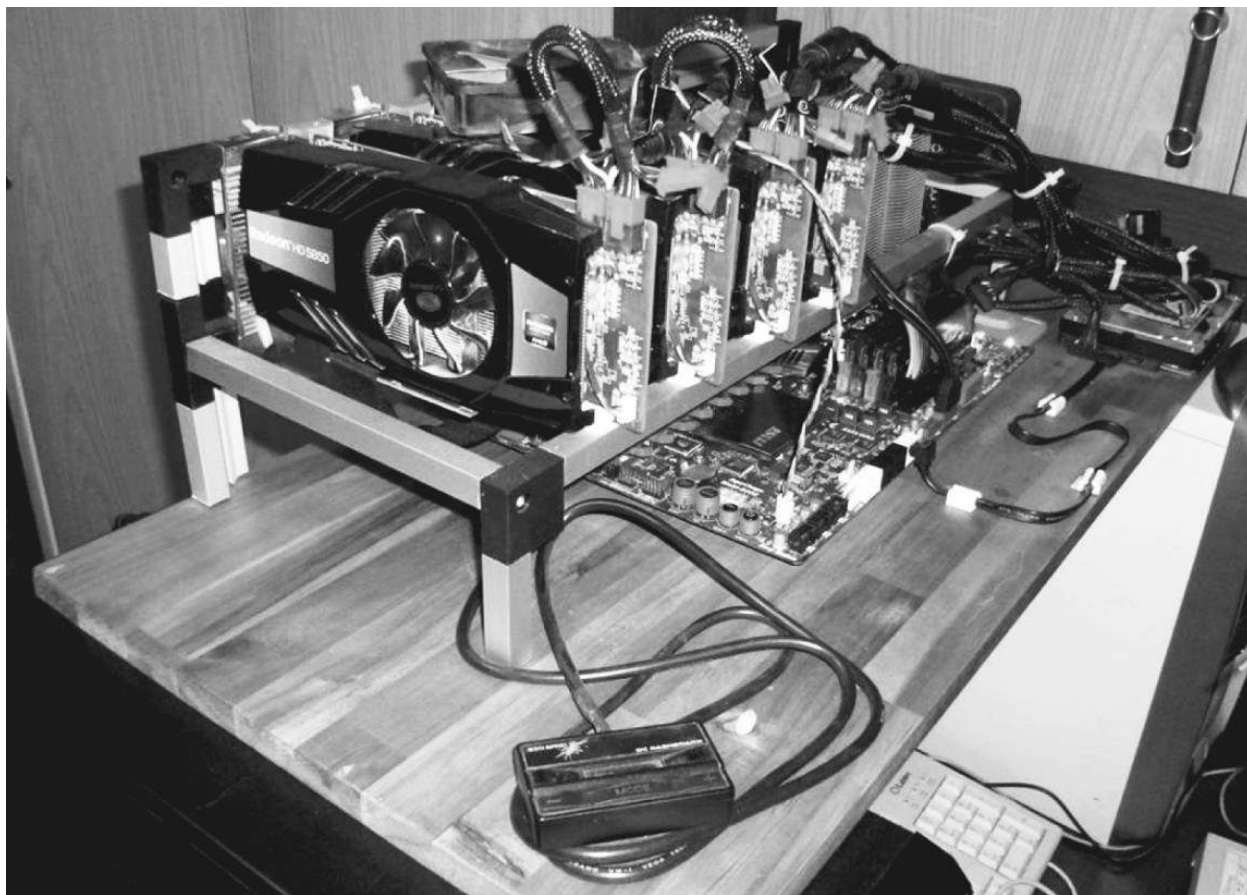


图5.7 一个用于比特币挖矿的家庭组装式GPU机架

资料来源: István Finta, bitcointalk.org

同时GPU也没有很好的冷却处理设置,尤其是当你把大量的GPU堆放在一起的时候,这个问题就尤为突出。设计显卡的时候并没有考虑如图5.7所示的这种堆放的情形,原始的设计场景就是在一台电脑、一个机箱、一块显卡运行做图形处理而已。

GPU也非常耗电,所以一台普通的电脑也会消耗很多电。由此引发的另一个缺点就是,你要么自己构建特定的主板,要么花大价钱购买可以搭载大量显卡的特定的主板。

一个非常高端的显卡经过超频之后可能使得运行速度达到200MH/s,也就是说,每秒可以进行2亿次哈希运算,这是用CPU不可能达到的一个数量级。但是即便如此,即使你将100块这样的显卡集成

在一起进行运算，根据2015年早期的比特币挖矿难度，仍旧需要运算几百年才有可能找到一个有效区块。因此，用GPU来挖矿基本上已经成为历史，但是在其他一些另类币的早期阶段还是很有效率的。

现场可编程门阵列挖矿

2011年左右，用于现场可编程门阵列(Field-Programmable Gate Array，简称FPGA)的硬件设计语言Verilog，第一次用于比特币挖矿。一些矿工开始用FPGA来代替GPU进行挖矿。

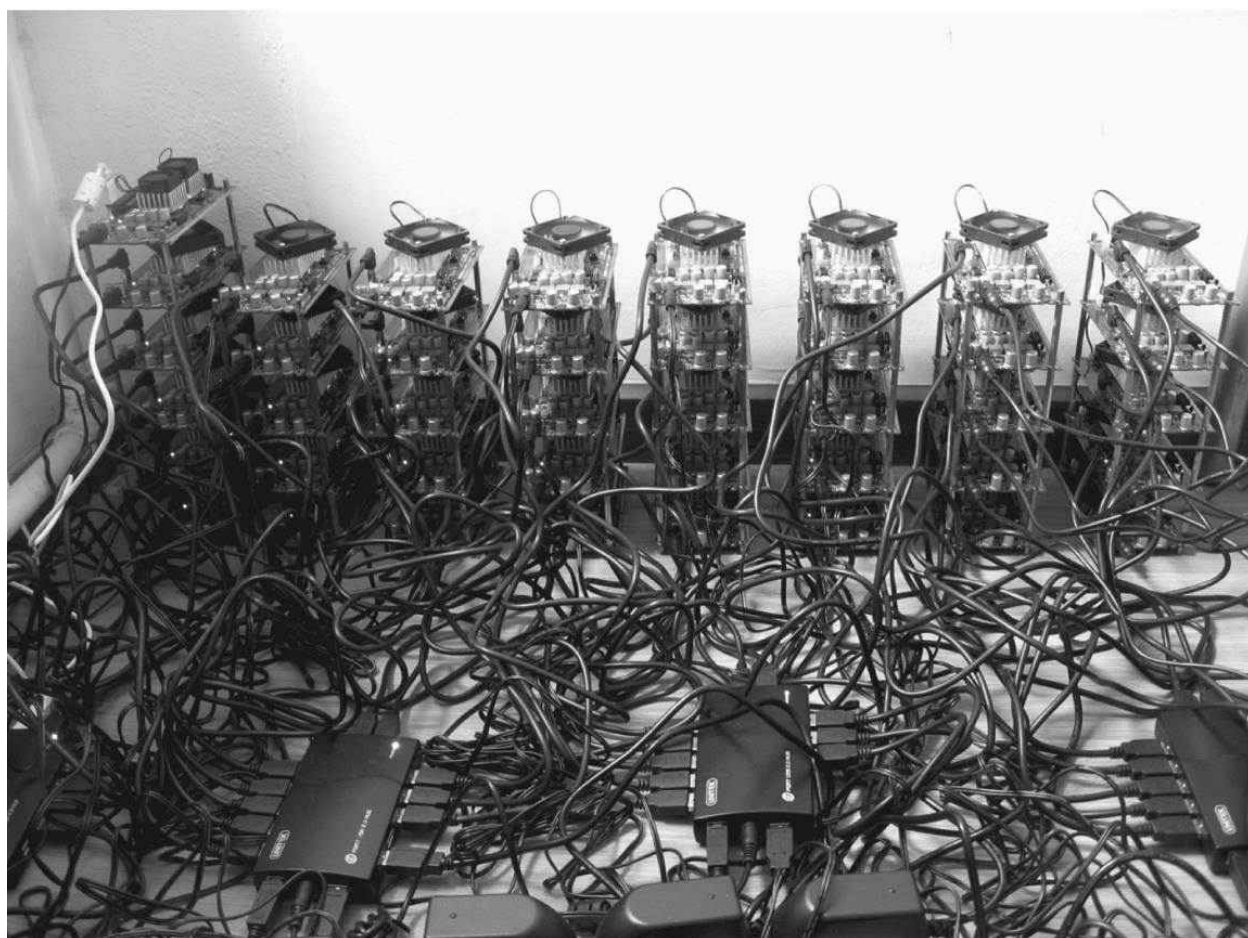


图5.8 家庭组装式FPGA机架

资料来源: Xiangfu Liu, www.openmobilefree.net

FPGA的工作原理是在追求定制硬件的最佳性能的同时，用户可以现场调试或者修改硬件参数。相比之下，常用的硬件是在出厂之前就设计好的，以后是无法更改定制而只能永远做同样的工作。

FPGA比GPU的性能好，特别是在数位操作（bit fiddling）方面FPGA很轻易就可以做到。FPGA也很容易冷却，不像GPU，FPGA理论上可以使用硬件板卡上的每一个晶体管进行挖矿运算。跟GPU一样，可以将很多FPGA堆叠在一起，通过一个中央处理单元来驱动所有的FPGA，如图5.8所示。总体来说，相比显卡堆叠，我们可以构建一个更加干净整洁的大型FPGA阵列。

精心使用FPGA可以使得运算速度上升到1GH/s，也就是每秒10亿次哈希运算。这显然比CPU或者GPU在性能上都有很大的提高，不过即使你有100块每秒运算1GH/s的FPGA板，在2015年早期的比特币难度之下，平均仍旧需要100年的时间才能找到一个有效区块。

虽然性能提高了，但由于以下几个原因，用FPGA挖矿的时代也非常短暂：首先，使用FPGA来挖矿其实更加困难——几乎需要一直超频使用——这远超FPGA供普通消费者而设定的频率。因为这个原因，很多人在用FPGA挖矿的时候经常看到各种报错和故障。其次，优化FPGA的32位加法处理上十分困难，而这在SHA-256的运算中非常关键。最后，FPGA在多数商店都买不到，而且相比GPU来说，只有少数人才知道怎么搭建FPGA并进行相应的编程。

最重要的是，即使在性能功耗比方面，FPGA相比GPU的提升也不是很高，这就使得用FPGA挖矿只是一个短期现象。尽管GPU挖矿的时代持续了大约一年，而FPGA存在的时间更加有限——仅仅存在了几个月，之后定制化的专用集成电路技术（Application Specific Integrated Circuits，简称ASIC）就诞生了。

专用集成电路技术挖矿

当今的挖矿市场主要被ASIC所主导。这些IC芯片（集成电路芯片）被设计、制造、优化，就是为了比特币挖矿这个唯一目的。有几个大型的供应商出售这些芯片，消费者可以买到不同种类的ASIC矿机——较大型但略微昂贵点的款式，或者更加小巧的，当然还有一些可以节省能源的环保型等。

设计ASIC芯片需要非常专业的知识，它们所需要的研发周期也比较长。尽管如此，比特币ASIC芯片的设计制造过程（从发现问题到制作出解决问题的芯片）出乎意料地迅速，甚至打破了芯片行业的业界纪录。但弊端是前几代的早期芯片的设计有许多缺陷，而且大多数芯片没有达到它们所承诺的性能指标。但现在的比特币矿机芯片技术，已经相当成熟可靠了。

到2014年年底，ASIC芯片的寿命十分短暂，原因是整个网络的运算能力不断地快速上升。绝大部分早期的ASIC芯片在6个月后就被淘汰了。在这段时间里，大部分的利润都是在早期实现的（后期几乎没有什么利润了）。矿工往往在ASIC芯片“保鲜期”的前6个星期可以实现整个利润的一半，这就使得芯片的出货速度显得至关重要。基于这个行业的不成熟，许多矿工经常遇到延迟出货的情况，有些芯片送到客户手上的时候已经快要被淘汰了。由于比特币的全网运算能力已经稳定下来，现在的比特币挖矿设备有比较长的寿命，但在早期，失望的客户对供应商的欺诈控诉的事件时有发生。

在比特币历史的大部分时间里，挖矿的经济效益对小矿工来说一直不是很好，这些小矿工们需要通过在线预定矿机，等待矿机生产送货，然后再开始挖矿赚钱。实际上，大多数情况下，由于不断增加的挖掘难度，很多人是一开始就注定要亏钱的。好在到2013年的时候，比特币价格大涨，彻底扭转了比特币矿工亏钱的状况。实际上，挖掘比特币一直

是一个很昂贵的投资，因为要赌注比特币的价格会上升，即使是在挖掘比特币中赚钱的那些矿工，如果能够把投资于挖掘设备的钱直接用于购买比特币，并在盈利时卖掉，这样他们的状况会更好些。

如今你仍然可以购买矿机，我们也不会劝阻你通过这种方式去了解比特币和加密数字货币，但是我们再次强调，这不是一个明智的生财之道。考虑到矿机运行所需要耗费的电力成本以及冷却成本，大多数ASIC矿机都无法靠挖矿来赚回成本。

如今：专业挖矿的天下

在今天，挖矿已经从个人领域转到了大型专业挖矿中心。为了保持竞争优势，运作这些挖矿中心的公司不愿意公布其运营细节。据猜测，这些运营者大量采购打过折的更新的功效更高的ASIC矿机而不是采购那些能够直接出售给个人的ASIC矿机来维持利润。

图5.9就是一个在格鲁吉亚运作的挖矿中心的图片。

展历程，我们就不难发现其与历史上的挖金矿有着有趣的相似之处。它们都开始于类似的淘金者热潮，很多年轻人和业余爱好者积极地参与其中。

比特币挖矿经历了一个逐渐演化的过程：从CPU到GPU，再到FPGA，最终达到现在的ASIC。而历史上的挖金矿则是从个人拿着盘子在沙里淘金，到一小群人用流沙槽来淘金，再到一群人用水冲刷金山来淘金，直到现代机械化露天挖矿（如图5.10）。比特币与黄金都从个人操作为主逐步演变为大公司专业运作。另外一个相似点就是，大多数的利润都被设备制造商拿走了，不管是黄金采掘设备还是比特币ASIC矿机生产商，而埋单的都是那些希望一夜致富的人。

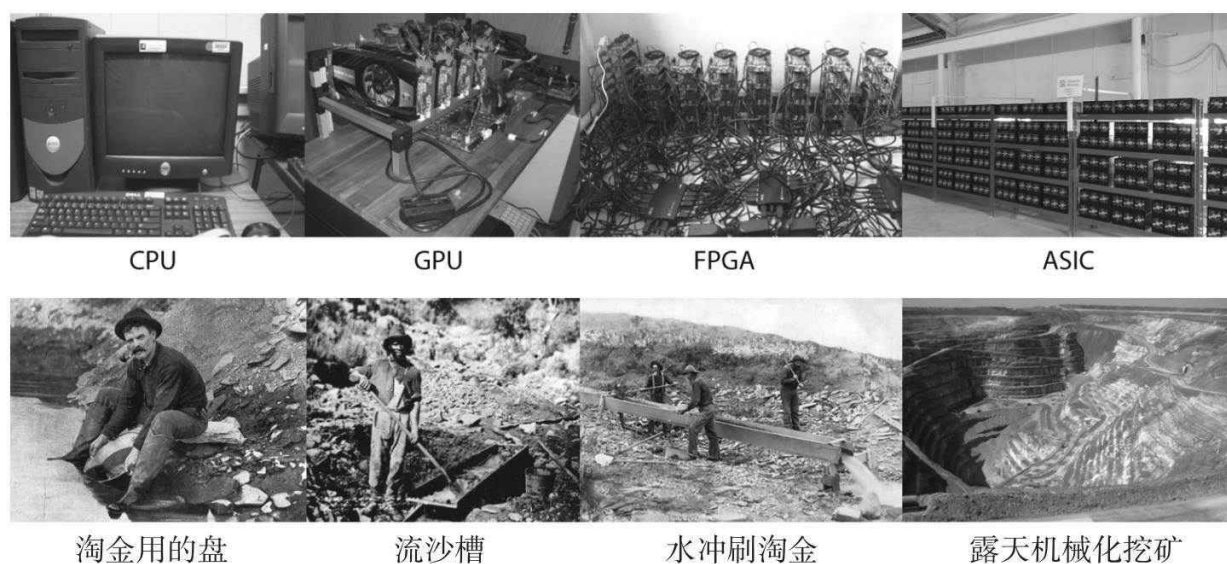


图5.10 比特币和黄金的挖矿进程

注：我们可以看到，比特币挖矿和黄金采掘进程有一个清晰的类似进程，两种活动在最初都对个人用户很友好，但是随着时间的推移，被大型公司采取集中式大批量运作控制。

未来

现在，用ASIC挖矿是唯一一种可以赚钱的比特币挖矿手段，但对个体矿工来说，是十分不友好的。人们不禁要问，未来会如何发展？小

规模矿工是否永远不可能再参与到比特币挖矿中？是否有办法把小规模矿工重新纳入挖矿体系中去？更重要的是，现在使用的ASIC和专业挖矿中心是否已经违反了比特币当初设计的初衷：一个完全去中心化的系统，在这个系统上里每个人都能用自己的电脑去挖矿。

此外，如果这已经违背了中本聪对比特币的最初设计，换成系统只允许CPU来挖矿是不是更好？我们将在第8章探讨这些问题，以及一些对ASIC不友好的替代方案。

自我循环周期

事实上，有一些规模较小的另类币已经使用了和SHA-256不同的解谜算法，但是它们的挖矿发展轨迹和比特币没有什么不同。我们将在第8章到第10章更深入地讨论这些另类币，但是请记住，ASIC的研发和生产有着比较长的时间周期，所以如果一个使用新的解谜算法的另类币（即使只是在SHA-256的基础上做一点修改），在有针对性的ASIC面世之前还是会有一段时间。通常跟比特币一样，其他另类币的挖矿发展也会经历从CPU到GPU，再到FPGA，或者直接到ASIC的过程（前提是这个另类币非常成功，比如莱特币）。

因此，小规模矿工的策略也许应该是尝试一些新的另类币，在它们的价值还没有足够大到吸引大型挖矿集团投资的时候，成为这些另类币的挖矿先行者，就跟黄金采掘的过程一样，小规模矿工可以去尝试那些还没有被证明储量的区域。当然，这也意味着先行者们将会面临一个重大的风险，也就是这些另类币有可能永远不会成功。

5.3 能源消耗和生态环保

我们看到大型职业化挖掘中心是如何接管了比特币的挖掘工作，我们也看到比特币挖掘与历史上的淘金热有多么类似。时至今日，金矿开采一直被环保问题所困扰，比特币挖矿虽然还没有达到那个程度，但它已经开始消耗大量能源，这已经成为热门话题。本节中，我们将着重讨论比特币挖矿的能源消耗问题，以及其对货币系统和地球生态的影响。

热力学限制

根据热力学里的蓝道尔原理（Landauer's principle, 蓝道尔是前苏联20世纪60年代天才物理学家），任何一个不可逆转的计算都会消耗一定的能源，逻辑上来说，这种计算也可以被认为是一种信息丢失的过程。蓝道尔原理特别指出，任何移位运算都会消耗一定量（ $k T \ln 2$ ）的焦耳，其中 k 代表玻尔兹曼常数（Boltzmann constant, 大概等于 $1.38 \times 10^{-23} \text{J/K}$ ）， T 代表芯片以开尔文为单位的温度， $\ln 2$ 代表2的自然对数，大约等于0.69。算下来每一个单位数据的运算会消耗一点点热量，这从基础物理学原理上提供了一个能源最低消耗下限。

这里我们不做进一步推导，大概的意思就是每进行一个不可逆的数位运算都会消耗一个最小量的焦耳，能源是永远不会被摧毁的，只会从一种形式转变成另外一种形式，在计算中所消耗的能源大多数都是从高等级的电能转换过来的，然后被转换成可以在环境中最终消失的热能。

作为一种密码学中的哈希函数，SHA-256就是一个不可逆的运算，我们可以回忆一下第1章里所说的，不可逆转是作为密码学哈希函数的一个基本要求，既然不可逆运算需要消耗能源，那么SHA-256作为比特

币挖矿的基本要素也是不可逆的，那么比特币的挖矿过程必定会消耗能源。蓝道尔原理中描述的能源消耗下限要远低于实际挖矿过程所消耗的电能，虽然我们目前无法使计算的能源消耗达到这个热力学原理中的最优消耗，但即使我们做到了，比特币挖矿也是要消耗能源的。

比特币挖矿是如何消耗能源的？这个消耗过程分三个部分，其中有些可能还不是很明显：

1.内涵能源。 首先，比特币挖掘设备需要被生产出来，生产时所用的原材料就需要被物理开采出来，然后要把这些材料通过一系列的生产流程转化为比特币挖矿专用的ASIC，这两个过程都需要消耗能源，这被称为内涵能源。在收到那些矿机的时候，你已经消耗了巨大的能源——当然包括物流过程中产生的能耗——即使这时候你还没有开启这些矿机！

可喜的是，随着越来越少的挖掘容量的出现，内涵能源的消耗就会降低。随着越来越少的人会去购买新的ASIC矿机，这些矿机被淘汰的速度也会减慢，那么相应的内涵能源也会在多年的挖矿中被摊销。

2.电能。 当矿机启动开始挖矿时，它就会消耗电能。根据蓝道尔原理，这一步肯定会消耗能源。随着矿机越来越高效，所消耗的电能也随之下降，但是根据蓝道尔原理这个消耗不能降为0，电能消耗将会伴随着矿工的挖矿生涯。

3.冷却。 比特币矿机需要被冷却，这是为了防止矿机出故障。如果在非常寒冷的环境中进行小规模挖矿运营，冷却成本会微不足道。但即使是在非常寒冷的环境中，一旦在一个很小的空间运行了足够多的ASIC，还是需要承担额外的冷却成本去解决散热问题。通常冷却挖矿机的耗能形式也是利用电力。

大规模挖矿

内涵能源和电能的消耗（每单位挖矿工作完成）会随着挖矿运营规模的增加而降低，设计和制造运行在大型数据中心的芯片本身单位成本会降低，同时由于不需要很多电源，你可以使得电力输送更加有效。

当讨论冷却问题的时候却恰恰相反，冷却成本会随着规模的增大而上升。如果要进行一个大规模的比特币挖矿运营，需要在一个地方运行大量的矿机，那就意味着空间比较小不易于散热。冷却成本会随着规模化而增加（每单位运算量），除非矿机运行的物理空间同等规模地增加。

能耗预估

整个比特币系统到底需要耗费多少能源？当然，我们无法做到精确统计，因为这是一个去中心化的网络，大量的矿机分散在各处，并且没有正式记录。但是有两种基本方法可以对比特币矿机所产生的能耗进行估算。根据2015年早期的比特币价格，我们可以进行一个快速的简单计算，我们必须强调一下，这个数字只是一个大概的估算，因为不管哪种方法，计算过程中所用的参数都是很难估计并且变化很快，这些结果只能是一个数量级上的估算。

自上而下

第一种是自上而下的方法。现在每一个区块奖励是25个比特币，大约值6500美元。也就是说，比特币体系平均每秒钟凭空产生11美元给矿工。

现在我们思考一个问题：如果矿工把所有的11美元都用在电费上，

他们可以买到多少电？当然，矿工通常并不会把全部的收入都用于电费，这是用于计算电费的上限。电价在各地的差异非常大，我们可以用美国的工业电价，大约每千瓦时（kwh）10美分的价格来预估，也就是每百万焦耳(megajoules，简称MJ)大概3美分。如果比特币矿工把所有的每秒11美元收入都用来支付电费，他们可以购买每秒367百万焦耳，消耗大概367 000千瓦时电力。

单位能耗和单位电力 国际单位制（SI）中，能耗的衡量单位是焦耳，电力的衡量单位是瓦特，1瓦特代表每秒钟1焦耳。

自下而上

第二种是自下而上的方法，通过观测每个区块的难度，了解矿工计算的哈希数量，并以此来进行估计。假设所有的矿工都使用最高效的矿机，我们可以推导出一个最低电耗。

目前，最好的商业化矿机的功效数值差不多是3GH/s/W^[1]。那就是，这样的ASIC矿机每消耗1瓦特的电力，可以进行每秒30亿次哈希函数运算。目前全网算力是350PH/s，也就是350 000 000GH/s。^[2]根据这两个参数计算，我们就可以知道目前基于这种矿机效率，每秒钟全网的矿机需要消耗117MW的电力。当然这个数值还没有包括所有冷却需要消耗的能耗以及芯片本身的内涵能耗。因为只是做一个能耗的下限估计，这么算是可行的。

结合上述两种方法，可以推导出比特币挖矿大概所耗电力，这是几百万瓦特（megawatt，简称MW）的数量级。

100万瓦特究竟是多少？为了便于直观理解，可以对比一下大型发电厂产生多少电力。世界上最大的发电厂之一，中国的三峡水电站的发

电总量是10 000 MW，一个普通的大型水力发电厂的发电总量一般是1 000MW。世界上最大的核电站日本柏崎刈羽核电站（Kashiwazaki-Kariwa）的发电总量是7 000MW，而平均来说核电站的发电量为4 000MW，而火电电厂的发电总量一般为2 000MW。

根据我们的估算，整个比特币网络大概消耗了一个大型电厂总发电量的10%。虽然这个数字已经相当惊人，但是和地球上其他的用电“大户”比起来，这个还算是小的。

比特币挖矿在浪费能源吗

比特币这种“浪费”能源的形式经常被人诟病，因为SHA-256的运算没有其他任何用处。但是我们必须认识到任何一种支付系统都需要能源和电力的消耗。就拿传统的货币来说，纸币印刷、ATM机器的运行、硬币分类机器、点钞机、支付服务系统以及运送现钞和金条的武装押运车，无一不在消耗各种能源。你也可以一样说这些能源的消耗除了维护整个货币体系之外，没有任何其他用处。所以，如果我们认可比特币作为一个有用的货币体系，那么支持比特币体系的能耗就不能认为是浪费。

当然，如果我们可以用更加节省能源的解谜算法来代替现在的比特币挖矿，同时确保货币的安全性，那自然更好。我们将在第8章讨论这个问题，然而我们并不知道这种可能性是否存在。

能源的循环使用

另一种使比特币更加环保的主意是，把挖矿过程中产生的热能进行二次利用，而不是让热能无谓地耗散在空气中。这种收集计算机运算所

产生的热能的模式被称为“数据火炉”（data furnace）。这个想法的原理是使比特币矿机挖矿产生的热能经过一种特殊供暖装置的转换，用来进行家庭供热，而不需要传统的电取暖器。这部分热能供给就成了比特币挖矿的副产品。这么做的效率其实并不比购买一个传统的电取暖器差。也许对于家庭消费者来说，使用一个“数据火炉”并不会比将供暖设备连上网络和电源插座更复杂。

这种方案也有一些问题。虽然矿机发热的效率和电取暖器差不多，但是它们本身比用天然气供暖的效率差很多。另外如果在夏天每个人都把矿机关闭（至少在北半球），那么比特币的全网算力将会伴随人类取暖需求而产生季节性变动。如果数据火炉方案真的推广开来，将会给比特币的共识机制带来很有趣的影响。

矿机的所有权也不明确。如果买了比特币数据火炉用于取暖，你是否拥有挖矿所获得的收入呢？还是出售设备的公司获取这部分收入？大多数人对比特币挖矿完全不感兴趣——有可能永远没兴趣——所以由出售这些设备的公司来获取这部分挖矿收入更合理。这也就意味着取暖器会以略微亏损的价格出售。这样一来，一些有创造性的用户可能会在购买了这些取暖器之后，对设备进行改造以使得他们自己可以获取这部分挖矿收入。这可能会引发令人难堪的数据所有权管理之争。

将电力转换成现金

长远来看，比特币产生的另一个问题是：它可以最有效率地把电力转换成现金。想象一下，如果比特币ASIC矿机是一个很容易购买到的商品，并且主要的挖矿成本是电力，这便意味着，提供免费的或低成本的电力将会面临被滥用的风险。

在很多国家，政府都有用电补贴，特别是对工业用电进行补贴。这

么做的原因是政府希望吸引工业投资留在本国。但是由于比特币提供了一种很好地把电力转换为现金的途径，这可能使得政府要重新考虑用电补贴的模式，以防它们补贴的电力全部被转换成了比特币。政府用电补贴的意图是，希望可以吸引那些对国家经济和人民就业有帮助的企业，但是补贴比特币挖矿也许并不能对这两点有所帮助。

更大的问题是全球有数以亿计的“免费”插座，分布在家、学校、酒店、机场以及办公大楼等。有人可能把挖矿设备接在这些地方挖矿，因为别人会为此支付电费。事实上，他们还可能会用过时的设备而压根不考虑升级，反正电费又不是他们支付。在全世界范围内监控这些用于比特币挖矿的“偷电”行为，是一个异常艰巨的任务。

[1] GH为gigahash,s为second,w为watt。——译者注

[2] 截至本书翻译的时间，全网算力已经增长到了1 200PH/s。——译者注

5.4 矿池

设想一下作为单个矿工。假设你花了辛苦赚来的6 000美元买了一台全新闪亮的比特币矿机，你所期望的性能是平均每14个月会找到一个有效区块（在2015年早期一个区块的奖励价值在10 000美元）。

考虑到电费和其他运营成本，矿机的平均收入期望值应该是每个月400美元。如果可以确定每个月都能获得400美元，那么购买一台矿机是合理的投资。但是别忘了，挖矿是一个随机过程，你不知道什么时候可以发现下一个有效区块。在找到有效区块之前，什么都赚不到。

高方差

从矿工第一年能找到有效区块数的概率分布上看，这个分布差异是很大的，期望值（也就是第一年能找到区块的平均数）是相当的低。因为发现区块的比率是一个很低的固定值，并且这个值和你上次发现一个有效区块所花费的时间完全没有关系，因而总的发现区块的期望值是以柏松概率分布^[1]。柏松分布是指，如果有N个独立事件，每个事件成功的概率是 λ/N ，当N接近于无限大的时候的成功概率分布。比特币挖矿中，尝试每一个临时随机数的行为实际上就是一种超小成功概率事件，所以即使对于小矿工来说，N的值也确实很大，这种近似类比是很合适的。

如果你期望每14个月找到一个有效区块（根据泊松分布可知 $\lambda=6/7$ 个有效区块/每年），则有超过40%的概率在第一年你不会找到任何有效区块。对于个体矿工来说，这可能是灾难性的。你在一台矿机上花费了数千美元，并且支付了很多电费来运行，结果什么都没有获得。第一年

能获取一个有效区块奖励的概率大概是36%，这也就意味着即使你的电费不高，你也就可能刚刚够支付电费。当然也有很小的概率可能会发现两个甚至更多的有效区块，这种情况下才有可能真的赚钱。详见图5.11。

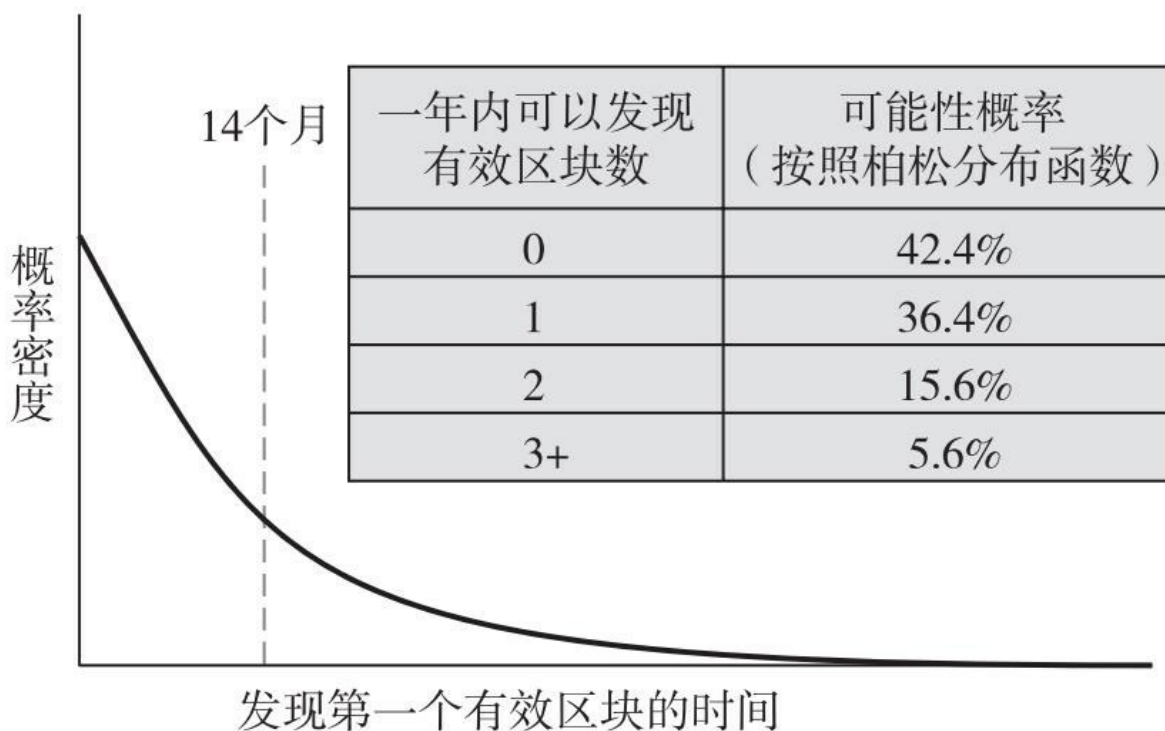


图5.11 挖矿成功的不确定性

注：假设全网哈希算力是不变的，平均发现一个区块的事件是14个月，对于一个小矿工来说这个成功概率的波动太大了。

这些数字只是一个近似估算，但主要的意思是，即使挖矿从期望值来说是合理的，也就是说，投资有足够的回报，但由于方差足够大以至于会有很大的概率什么都得不到。对于一个小矿工来说，这也就意味着挖矿就是一个赌博游戏。

矿池

历史上当小商人遇到大风险的时候，他们会自发组建一个互助保险

公司来降低风险。比如，农夫会自发地聚在一起形成一个协议，如果任何一个个体农夫的谷仓不小心被烧掉了，那么其他的农夫可以把他们的利润拿来和这个不幸的农夫分享。那么对于比特币的小矿工是否也可以用类似的方式来降低风险呢？

矿池应运而生——矿池就是一个比特币矿工互相之间的保险。一组矿工可以形成一个矿池共同进行挖矿，并指定一个币基接受人。这个接受人就是矿池管理员。所以不管是谁最终发现了一个有效区块，矿池管理员将会收到这个区块的奖励，继而根据每个参与者所贡献的工作量按比例分配给所有矿池的参与者。当然，矿池管理员可能从中分一部分来作为矿池管理服务的收入。

假定每个人都信任这个矿池管理员，这样的分配安排可以极大地降低矿工成功寻找有效区块的概率波动。但是矿池管理员如何知道矿池里每个成员实际上到底贡献了多少工作量呢？同时他又是如何去分发收入的呢？很显然，矿池管理员不希望是靠每个成员的申明，因为他们可能会虚报自己的工作量。

挖矿工分

对于这个问题，我们有一个简洁的解决办法。矿工可以通过输出挖矿工分（**mining shares**）来证明他的工作量，工分就是那些接近有效区块的区块。比如目标值是个前面67位是零的数字，输出的哈希值必须低于这个目标才算有效。在寻找这个哈希值的过程中，矿工可能找到其他一些区块，它们的哈希也有许多零，但达不到67个。矿工可以用这些区块来证明他们确实在工作（见图5.12），一个合格的工分可能要求40~50个零，取决于矿工所加入的矿池的要求。

9D1842A2A98DEDE34E00F6B8406AED0CE11BDC906C6DB6E23BCD9DE35DC4C339
86006DC06851F801FF0322E4CB92959DB619F19A03415B0C8FE131968005B9DA
00000000004D4120FD53C6CE8F013367209E905F4AE4D7837FFCFAA22B95CEDF
60E9D45D86FA3AE285615A3972E9F85C68FEA07611830F49ED15EEE1460E83A4
00000000007EF3D0D4479C9FB96FF100601618AD56BD240EF762B1B6842D1CF5
44AEE951CD30363A0A750C81CDC4BC0D3427DACA1C878A489120EB92430866F7
D048C51CA7EA5E6B61F6B40E739F9F35E2C653A37BE7D3EA2474F5E7777C8790
00000000000000001EB96F35E74E9B0F84BC921D52EDC878A754658F23313E86
1289F7CFA4A86DEBB743D2B94AAD0A916A9282FDCA05B70E72C627FE5A592959
561BBB9E8AAC2B1DDE1E163DA1E4F05BC1A9B1E92B04DCE834A6EB827C5E2E5B
000000000082D602D87B67A42ED2BF763E92A76BE90F76A9CA71AB958EB7657A
FD639DC38BB5279885F0FC42E7FD92D37ABD7FEAFD828CEDA2731CD781DC77D7

图5.12 挖矿工分

注：矿工不断尝试去发现哈希值低于目标区域的有效区块。在这个过程中他们会发现一些区块的函数值比目标值少了几个0——但是已经是非常稀有的，这证明了他们确实在进行繁重的运算工作。在这个图中，浅色阴影的哈希值就代表工分，深色阴影部分是有效区块的哈希值。

矿池管理员也会作为参与者之一运行比特币节点，收集交易并组装区块。他会把他自己的接收地址放在币基交易里，然后把这个区块发给所有矿池里的矿工们。矿工们收到后会在这块上面开始挖矿，最后递交工分来证明他们确实进行了运算工作。

当矿池一个成员找到了一个有效区块，他会把这块发给矿池管理员，然后管理员会根据大家的工作量按比例分配奖励。发现这个有效区块的矿工并不会因此获得特别奖励，所以如果其他矿工的工作量更大，那么其他矿工就会获得更多的奖励，即使他们并不是真正发现有效区块的人。如图5.13。

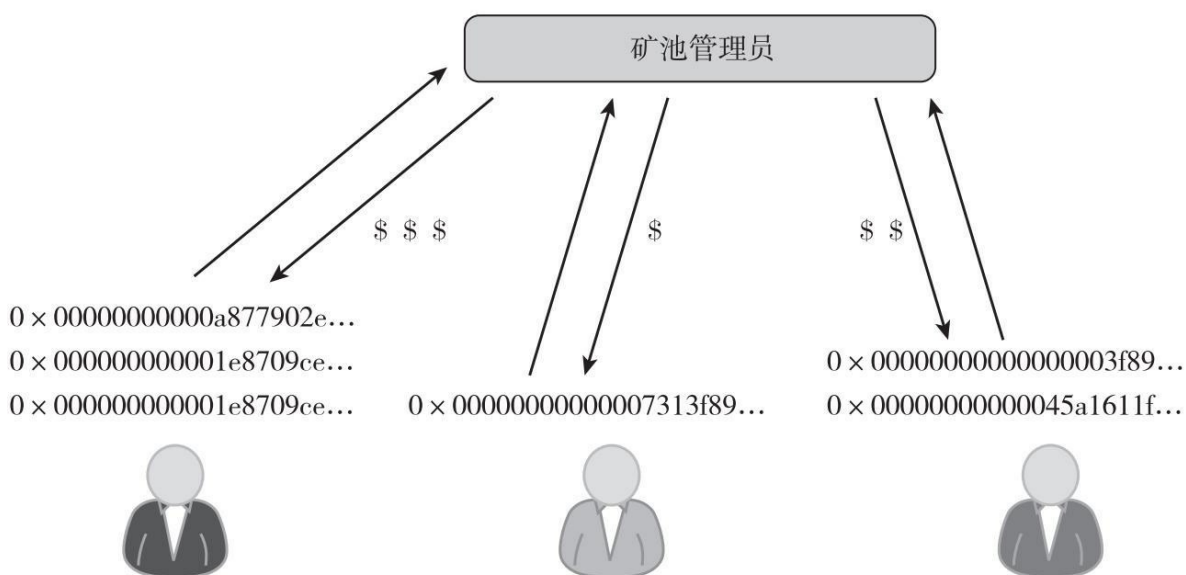


图5.13 挖矿奖励

注：图上三个矿工在同一区块上挖矿。他们最后的奖励是根据他们工作量的大小来决定的。即使是右边那个矿工找到了有效区块，但左边那个获得了更多的奖励，因为他的工作量更大。找到有效区块的矿工并没有收到特别奖励。

矿池管理员如何分配奖励的方案有好几种，我们将会探讨一下最常见也是最简单的两种，也有其他一些方案被不同的矿池使用，但这两种基本上可以解释奖励方案之间的权衡选择。

工分分红

在这个模式里，管理员会对每一个超过特定区块难度的工分发放固定的奖励分红。在这个模式里，矿工在发送工分之后，管理员马上就会对其支付奖励，而不需要等到整个矿池发现一个有效区块。

从某些方面来说，工分分红的模式对矿工是最有利的，他们可以确保每次发现一个工分的时候都有一定的收入，而管理员其实担当了所有的风险，因为无论矿工是否找到有效区块，他都必须按照工分支付奖励。当然，和其他模式相比，因为风险的增加，管理员也会收取更高的管理费用。

这个模式的问题是，矿工没有动力把有效区块提交给管理员。也就是说，即使把有效区块丢弃了，他们也会得到同样的奖励，但对整个矿池来说是个巨大的损失。一个恶意的管理员可以作为矿工参与另外一个矿池，用这个方法攻击另一个竞争对手，让他的矿池无法维持下去。

按实际比例分红

在这个模式里，不是按照工分分发固定分红，每个工分所能得到的分红，取决于整个矿池是否可以找到一个有效区块。每次找到一个有效区块，区块奖励（25个比特币再加上交易费）会按照每个矿工的 actual 工作量按比例分配。

在这个模式里，矿工仍然会承担与矿池风险成一定比例的风险。但是如果矿池足够大，发现有效区块的概率波动会相当低。按实际比例分配的模式大大降低了矿池管理员的风险，因为只有矿池发现有效区块的时候才会支付矿工奖励。这也解决了工分分红模式的问题，矿工有动力把有效区块提交给管理员，因为只有那样他们的奖励才会被相应发放。

相比工分分红模式，这个模式略微增加了管理员的工作量，他要校验、计算和分配奖励。

矿池跳换

即使只有这两种矿池运营模式，我们可以看到矿工有动力去时不时地进行矿池跳换（pool hopping）。比如，一个按实际比例运行的矿池很快发现有效区块时，不管有效区块被发现的间隔是多久，管理员都会快速支付矿工奖励。

一个聪明的矿工可能尝试在挖矿周期的早期（也就是上一个区块刚刚被发现），在按实际比例分红的矿池中挖矿，这个时候的奖励可能相

对比较高，然后只在周期的后期切换（“跳”）到一个工分分红模式的矿池，这个时候按实际比例分红的矿池收益可能相对较低。这样导致的结果就是按比例分配的矿池可能无法运行。实际上更加复杂的方案可以防止这种矿工行为，比如“根据最近N个工分提交的结果才分配”是比较平常的做法，但即使这些方案也有可能诱发矿工跳换的行为。如何设计一个矿池方案以使其更好地防止这种行为，仍旧是一个有待解决的问题。

历史和标准化

矿池兴起于2010年比特币的GPU时代，并迅速变得十分受欢迎。道理很简单，因为它降低了矿工的概率波动风险。时至今日，矿池已经发展得十分先进。已经有很多矿池管理协议应运而生，甚至有人建议这些矿池管理协议应该被标准化，并且作为比特币本身的一部分。就像比特币的点对点网络协议一样，这些矿池协议也提供了一种特定的通信应用程序编程接口(Application Programming Interface, 简称API)，用于矿池管理员与每个矿工交流分派工作和矿工们递交工分给管理员。获取有效区块模版（`getblocktemplate`，简称GBT）就作为一种标准化的矿池协议放进了比特币改进方案（Bitcoin Improvement Proposal, 简称BIP）之中。一种被称为层（stratum）的竞争协议，目前在实际中运用很广泛，就是一份BIP。不像比特币本身的协议，从事存在多个互不兼容的矿池协议没有造成太多的不便。每个矿池可以选择它们喜欢的协议，然后让市场来判定孰优孰劣。

有些挖矿机甚至把这些协定放进了硬件，但这最终会对限制这些矿机的灵活性有所限制。然而这使得购买矿机加入矿池变得异常简单。只需要把矿机插上电并连接上网络，选择一个矿池，然后这个矿机立刻就会接受该矿池的指令开始挖矿，并把电力消耗转变成收益。

51%的矿池

2015年早期的时候，绝大部分矿工都通过加入矿池来挖矿，只有很少的矿工还在单独挖矿。而在2014年6月，网络里最大的矿池 GHash.IO，曾经变得如此巨大，其算力甚至超过了比特币全网算力的50%。主要是因为这个矿池给矿工优厚的奖励，以至于大家都想加入。

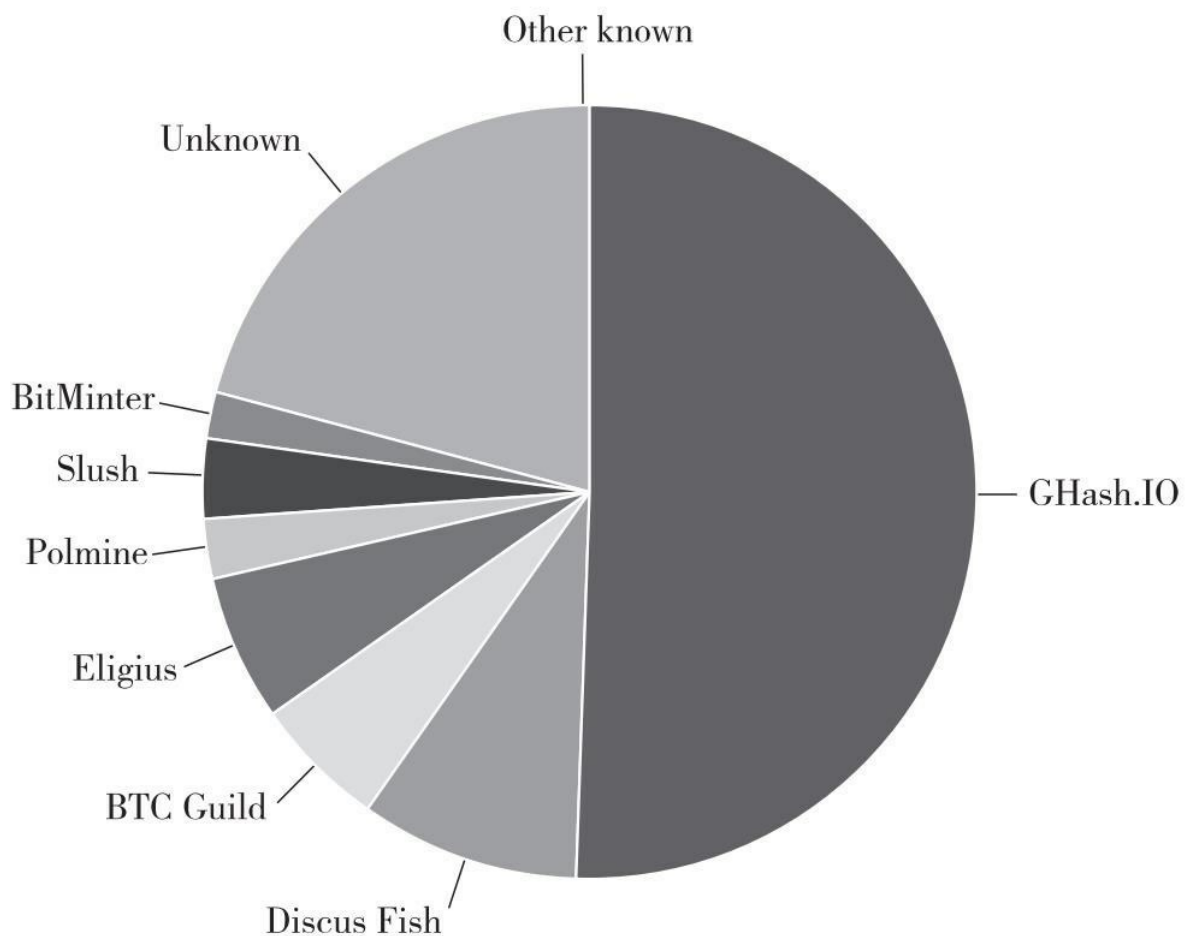


图5.14 (a) 矿池的算力分布

资料来源: blockchain.info (2014年6月)

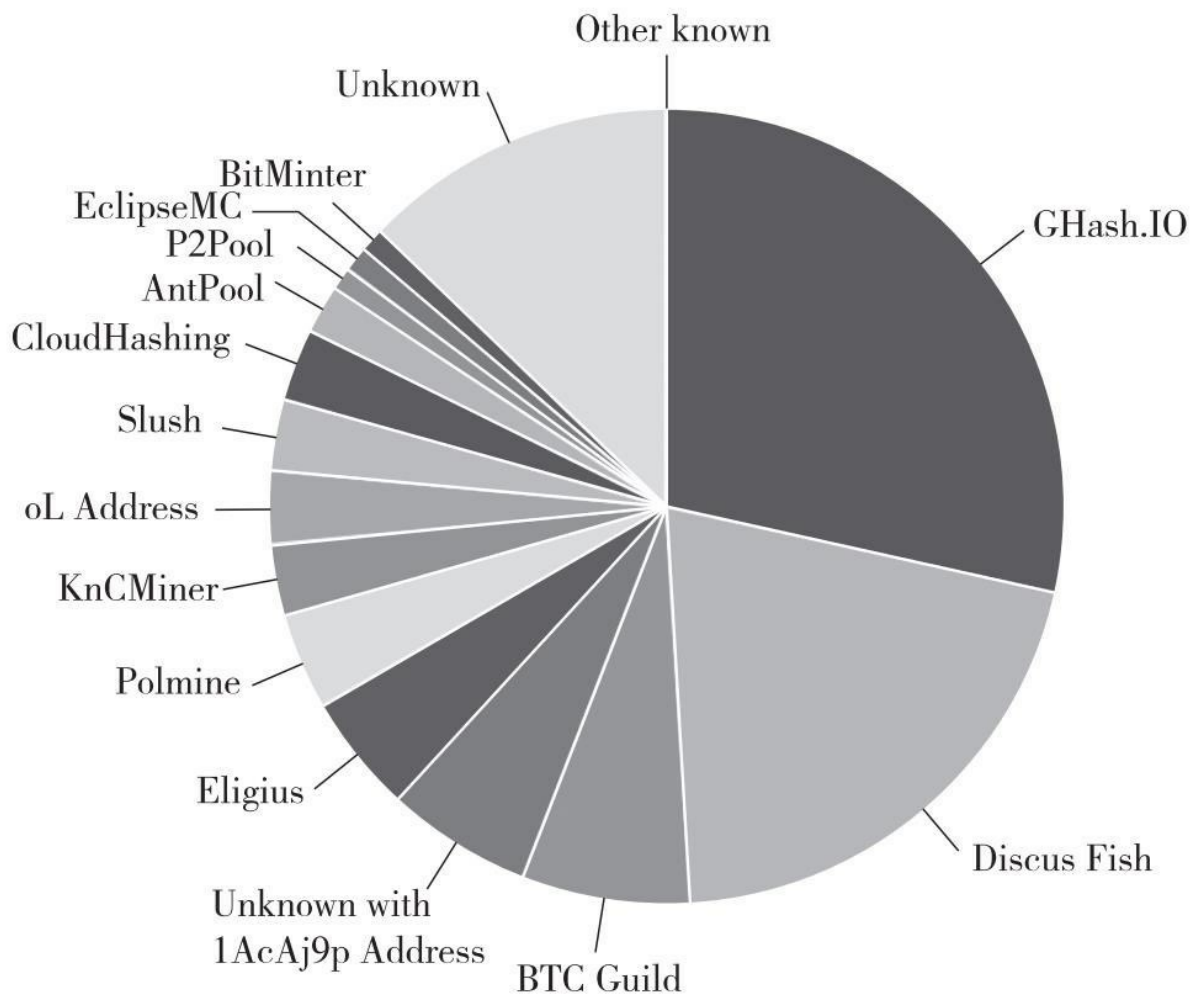


图5.14 (b) 矿池的算力分布

资料来源: blockchain.info (2014年8月)

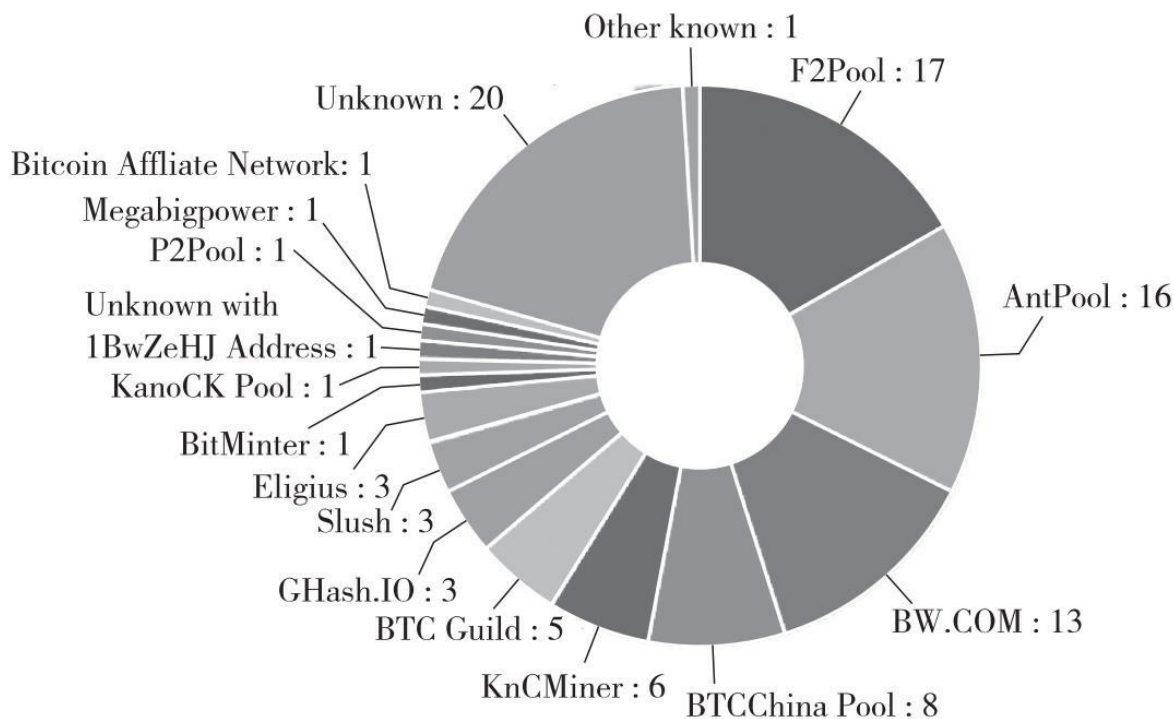


图5.14 (c) 矿池的算力分布

资料来源: blockchain.info (2015年4月)

但这也是比特币社区一直所担心的，也导致了对GHash的反击。到了8月，GHash不再接受新用户而主动下调了一些比例。即便如此，两个矿池依然掌控了整个网络一半左右的算力。

到了2015年4月，形势改变了许多，至少从表面上来看变得不是那么集中。但一个矿池掌控51%的算力依然是社区里一个令人担忧的问题。然而GHash遭受的负面的公众效应让很多矿池意识到这个问题，并尽量避免增长得过大。随着新的矿工加入市场，标准化的协议使得矿池之间的切换更加容易，矿池的市场份额一直在变动。矿池在长期如何发展，目前还不明朗。

无论如何，矿池有可能会掩盖这样一个事实：实际上的算力集中在几个大的挖矿机构手上，这些大的机构可以同时参与多个不同的矿池以掩盖它们的真实规模。这种做法被称为“洗算力”（laundering hashes，类

似于洗钱)。因为矿池的原因，发现洗算力变得非常困难，这也使得外人无法知晓矿机的实际物理控制有多么集中。

矿池是有益的吗

矿池的好处在于矿工挖矿变得更加容易预测，也让小矿工更加容易参与。如果没有矿池的存在，挖矿效益上的概率波动会让小矿工承受不起。

矿池另外的一个好处在于，每一个矿池都有一个中心化的矿池管理员在网络中组装区块，所以网络更新变得更加容易。只要更新管理员的软件，即可更新所有矿池成员的软件。

当然矿池的一大问题是中心化管理。矿池管理员实际掌握了多大的算力是一个问题。当然，理论上一个矿工如果觉得管理员权力太大，可以自由地选择离开，但实际中有多少矿工会这样做还不清楚。

另一个坏处是减少了比特币网络上校验全部交易节点的数量(全节点)。以前，无论大小，所有矿工都必须自己运行一个全节点。他们要存储整个区块链，并校验每个交易。现在他们把这项工作交给了矿池管理员。这也是我们在第3章中提到的：整个网络中进行校验交易的全节点的数目在下降。

如果你对矿池的中心化模式感到不安的话，你可能会问：我们是否可以重新设计挖矿的流程，这样我们就不需要任何矿池，大家必须自己进行挖矿。我们会在第8章中探讨这个问题。

[1] 柏松是18世纪法国数学家，概率学奠基人之一，柏松分布被广泛用于各个领域的概率分析。——译者注

5.5 挖矿的激励和策略

我们在这一章花了很多篇幅讨论作为一个矿工的主要挑战：买到好的硬件、找到廉价的电费，然后尽快开始运行，然后期待一些好运气。不过在挑选一个区块开挖之前，每个矿工都需要做一些策略上的选择：

1.需要包括哪些交易？矿工可以选择将哪些交易放进他的区块里。默认的规则是选择那些交易费比较高的交易。

2.对哪一个区块进行挖矿运算？矿工可以选择在哪个区块上进行挖矿。默认的做法是在最长的那条区块链上继续挖下去。

3.在同一高度的多个区块中做选择。如果两个不同的区块在同一时间被宣布发现，这就造成了一个区块的分叉，每个区块都是可以被延续下去的，因为它们都符合最长区块链原则。矿工必须选择其中一个区块接龙下去。默认的做法是选择最先被监听到的那一个区块。

4.什么时候宣布新的区块？当矿工找到一个有效区块之后，他们要决定什么时候向比特币网络宣布这一个区块。默认做法是立刻宣布，但他们也可以选择等一下。

矿工其实面临很多决定。每个决定都有一个默认策略，直到这本书撰写之时，绝大多数的比特币客户端都是按照该默认策略运行的。非默认策略也有可能使得挖矿收益更高，很多人积极研究如何找到这样的策略。让我们来看看几种可能有别于默认策略的做法，这些做法可能使得挖矿收益更高。在接下来的内容中，我们假设一个运行非默认策略的矿工掌控一定的比特币网络挖掘市场份额，设为 α 。

分叉攻击

最简单的攻击就是分叉攻击（forking attack），这是一个显而易见的获利方式——重复支付。一个恶意的矿工给一个受害者鲍勃发送了一些比特币来购买其服务和货品。鲍勃等到这笔支付交易被放进了最长链之后，甚至还等到了6个证实的时候确认支付安全之后，才开始发货或者提供服务。

现在这个矿工开始跳到前一个区块上开始重新挖矿——就是在那个包含他给鲍勃的支付交易区块之前的那一块。在这个分叉的区块链里，他插进了另一个替代交易——或者进行一个双重支付——把那些已经支付给鲍勃的比特币重新发送回自己的地址里（见图5.15）。

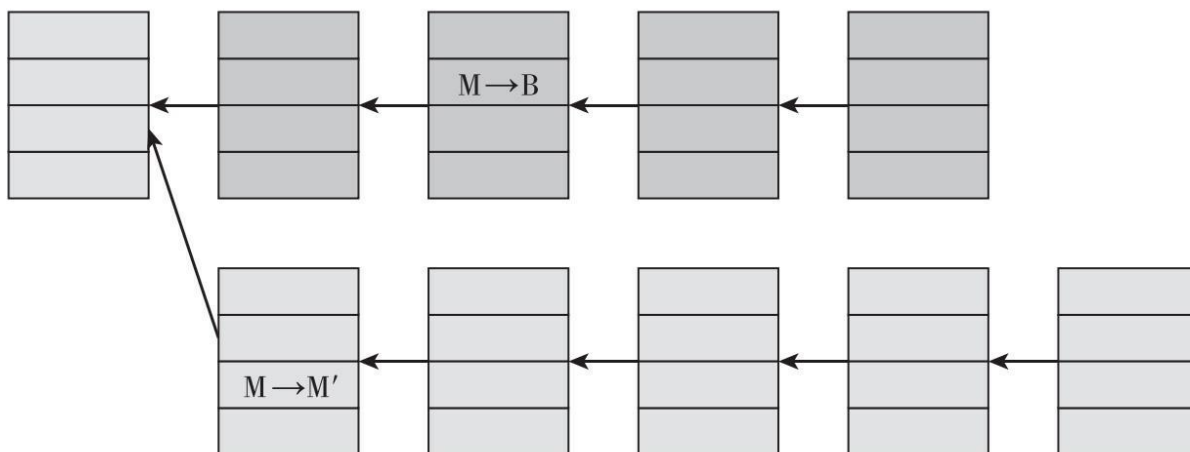


图5.15 分叉攻击

注：一个恶意的矿工给受害者鲍勃发送了一些比特币来购买其服务和货品。然后这个矿工进行了一个分叉攻击，创建了一个包含冲突交易的更长的分叉，在新的共识链中给鲍勃的支付就变成了无效的交易。

想要这个攻击成功，被分叉的区块链必须要覆盖当前最长的一条链，一旦这个情况发生，支付给鲍勃的交易就不再存在于共识的区块链里。如果这个矿工掌握占优势的哈希算力的话，也就是说 $\alpha > 0.5$ ，这种攻击就会成功。也就是说，即使有大量的随机变数，这个分叉最终会变成最长的一条链，也就是正当有效的共识链。甚者，因为这些币已经被

用过了（在新的共识链上），这笔支付给鲍勃的交易永远不可能再回到区块链上了。

51%是必要的吗？ 如果 $\alpha > 0.5$ 的话，发动一个分叉攻击是很有可能发生的。但在实际中，用稍低的算力也可以发动一个那样的攻击，因为有类似于网络拥塞之类的其他因素。在主链上挖矿的其他矿工会因为一个正常的原因产生一些过时的区块——因为有网络延时。但是一个中心化的攻击者本身则不会有这个延迟，他可以进行更快速的通信并且生成更少的过时区块，这可能会节省1%甚至更多的算力。

拥有近乎50%算力的攻击者可能需要花很长时间才可能成功，因为有随机性。算力超过50%越多，攻击就会变得越容易也越有效。人们经常讨论51%的攻击，是因为51%是一个分水岭，超过51%的时候分叉攻击就会成为可能。实际上，这种攻击的成功概率是呈梯度变化的。

可操作的对策。 我们不清楚分叉攻击在现实中是否一定成功。因为大家可以觉察到这个攻击，社区可以对此做出决定，即使分叉链更长也可以拒绝接受。

攻击和币值（exchange rate）。更加重要的是，这种攻击可以摧毁大家对比特币的信心，比特币的拥有者们就想要把资产转移出去，以至于比特币价格崩溃。因此，虽然一个具有51%算力的攻击者可能会在短期内利用双重支付进行欺骗并获得额外的收益，但是从长期来看，其实他们这么做造成的损失可能更大。

所以发动这种攻击的人其实是想通过打击信心来摧毁比特币。有点类似于邦德电影里的反派想要对诺克斯堡里的所有的黄金进行辐射污染，使其变得没有价值一样，这类攻击被称为金手指攻击（Goldfinger attack）。这种攻击者的目的可能就是摧毁整个货币，可能是由于他可以通过要么做比特币空头交易，要么拥有大量的竞争货币而获益。

通过贿赂来进行分叉攻击

通过购买足够多的矿机来控制大部分的算力，是一件非常困难而且昂贵的任务。但可能还是会存在其他简单的方法来进行分叉攻击：相比直接购买算力以获取超越所有其他人算力的昂贵做法，贿赂那些有能力的矿工来为你来工作也是可能的。

有几种贿赂其他矿工的方法。其中一个方法是“系统外的”（out of band）——可能找到一些矿工然后直接用现金来贿赂他们。当然一个更加聪明的办法是创建一个新的矿池，然后提供更好的奖励来吸引其他矿工来加入，即使矿池运行可能因此而亏损。虽然这种奖励不可能长期维持下去，但是可以维持足够长的一段时间直到可以发动一个成功的分叉攻击，然后获利。还有一种方法是在你的分叉区块链里留下足够多的“小费”，多到足以让其他矿工离开最长链来加入你的分链，矿工们希望你的链成为最长的链，这样一来他们可以收取你留下的小费。

不管是哪种贿赂的方式，核心思路都是一样的：有别于直接获得大量算力，攻击者去贿赂那些已经拥有算力的人，让他们帮助自己分叉出另外一条最长的区块链。

可能矿工们并不愿意去帮助一个攻击者，因为这么做会危害整个货币的价值，而他们已经在此之上投入了相当多的资金和矿机。从另一方面看，虽然矿工们作为一个整体可能希望保持货币的价值，但是他们可能做不到一致行动。个别矿工可能会因为短期利益，将个人利益置于集体利益之上。从经济学的角度来看，那就是个经典的“公地悲剧”了。

这些假想在现实中未曾发生。贿赂攻击是否可行，这依旧是一个悬而未决的问题。

临时保留区块攻击

假设找到一个区块之后，默认的做法是你会立刻向全网宣布找到的区块。但是如果你想进行一个临时保留区块攻击(temporary block-withholding attacks)，你也可以不立刻宣布，然后在这块上面继续挖矿，期望你可以在其他矿工找到下一个区块之前连续找到两个有效区块，在整个过程中秘密地保留你所发现的区块。

如果你已经拥有两个公共区块链上超前的秘密区块，那么全网剩下的矿工所做的挖矿努力都会被浪费，其他的矿工都会在他们认为最长的链上继续挖矿，一旦他们宣布他们找到了一个有效区块，你可以立刻宣布你所秘密保留的两个区块，这样你的区块链立刻变成了最长的有效链，而其他辛苦挖出来的区块马上就变成了一个孤块而被丢弃（见图5.16），你的这种行为被称为自私挖矿（selfish mining）。通过使网络上的其他矿工浪费算力计算出来的区块瞬间过期，可以有效地增加你的挖矿获利。

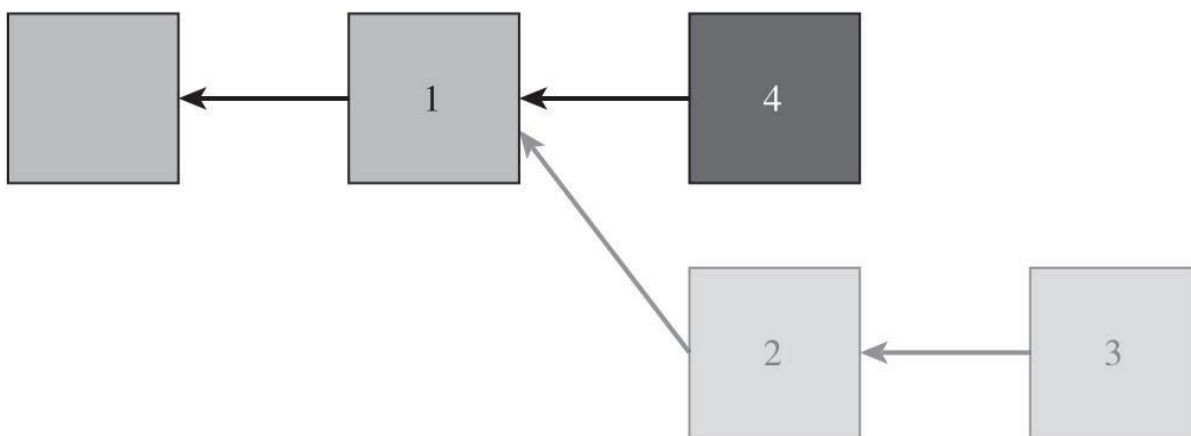


图5.16 自私挖矿图示

注：图中显示了其中一种攻击方式。（1）攻击之前的区块链。（2）攻击者挖到的区块，保留着，在此之上继续挖矿。（3）攻击者运气很好，在全网其他矿工之前发现了第二个区块，并继续保留。（4）非攻击者找到了一个区块，并进行广播。攻击者立刻广播他所保留的两个区块，使得区块4变成了孤岛，浪费了其他人之前所用的算力。

这里面的关键是你需要运气好到连续发现两个区块，风险在于你只领先了一个区块，其他人就已经向网络宣布发现了一个有效区块。如果这种情况发生，你必须立刻宣布你的秘密区块，这叫造成了一个区块的分叉，每个矿工都需要选择哪一个区块继续挖下去。当然，你希望大部分其他矿工最早监听到你的区块并在上面继续挖矿。由于这种攻击的有效性严重依赖你赢得这个竞赛的能力，所以网络位置至关重要。你可以尝试跟所有的节点建立链接，以使得你的区块可以第一个到达其他的节点。

假设只有50%的机会可以赢得这个竞赛，在 $\alpha > 0.25$ 的情况下，自私挖矿可以比默认策略更有收益。如果 $\alpha > 0.333$ ，即使你输掉每一个这种竞赛，仍然可以获得更高的收益。这种攻击的存在是令人震惊的，原来大家都相信如果没有很大的算力——比如 $\alpha \leq 0.5$ ——不会有比默认策略更有利的挖矿策略。所以，即使某个矿工控制的算力低于50%，也是有可能通过切换到其他的挖矿策略来获取更多的收益。

到2015年为止，临时保留区块攻击仅仅是理论上的，在实际中并没有观察到这类攻击事件，自私挖矿则很容易被检测到，因为这种策略会增加同时宣布区块的概率。

黑名单与惩罚分叉攻击

如果一个矿工想把一个来自地址X的交易列入黑名单，换句话说，他想冻结从该地址出来的钱，让这些钱变得不可用。或许他想用这个办法来敲诈勒索一笔钱，或许他们之间有仇，还有可能是政府执法部门认为那些地址有问题，需要矿工的配合来冻结这些币。

传统观点都认为在比特币里这种黑名单没有办法有效施行。因为即使有些矿工会拒绝把交易放进区块链里，其他一些矿工可能会。如果你

真的想把一笔交易列入黑名单，你可以尝试其他一些更加激烈的手段，比如，惩罚分叉（punitive forking），你可以宣布拒绝在包含来自该地址的交易的区块链上工作。如果你拥有大部分市场运算能力，那应该足以保证这个黑名单上的交易永远不会被公布。确实，在这种情况下，其他矿工很有可能不会再试图把这笔交易放入区块链里，因为这么做有可能使得他们自己的区块链被分叉，这会导致他们发现的区块被删除。

羽量级分叉

如果没有很大的算力，上述的几个分叉攻击在现实中都不太可能实现。如果你宣布拒绝接受包含某些特定交易的区块链，但这条链被网络上的其他矿工所接受并形成最长链的话，你就会发现自己被永远排除在共识链之外（这就是一个硬分叉），所有你做的挖矿工作统统浪费了。更加糟糕的是，黑名单上的交易仍然存在于最长的区块链上。

换句话说，考虑到还有其他矿工的存在，用惩罚分叉把特定交易放入黑名单的手段并不可靠。然而，有另一个更明智的方法可以做到这一点。与其一看到从地址X里出来的交易就宣布你会进行永久分叉，不如宣布你将会尝试分叉，但过一段时间你可能会放弃封杀的尝试。例如，你可以宣布：当k个区块证实了从这个地址出来的交易是正当的时候，你便会回到最长链。[\[1\]](#)

如果你在一个区块证实后便放弃，把那笔从地址X出来的交易成功封杀的概率是 α^2 。原因是你必须要在其他矿工找到下一个区块之前找到连续两个区块，这样才能成功地丢弃那个包括地址X交易的区块。 α^2 是你连续找到两个区块的概率。

α^2 这个概率看上去不是很好。就算你掌控了20%的全网算力，也只有4%的成功概率来封杀那笔你不希望出现在区块链上的交易。但这已

经不错了，至少你还有可能说动其他矿工来加入你。只要你把你的计划公开了，其他矿工便会知道：如果他们胆敢把这个来自地址X的交易加入自己的区块，便有 α^2 的可能会丧失自己已经发现的区块〔被你的羽量级分叉攻击（feather forking）所消灭〕。只要他们不是有很强的主观意愿把这个交易包括进来并且这个交易没有很高的交易费，他们可能更愿意规避那 α^2 失掉过往挖矿奖励的风险，而不是获取那笔交易费。

这就演化为：其他挖矿者经过理性的思考，将决定加入你对X地址的封杀行动，这样你便可以成功地封杀X即使 $\alpha < 0.5$ 。所以这个攻击要想成功，重点在于确保其他矿工相信你将会进行分叉攻击。

逐渐转移到用交易费来奖励挖矿

直到2015年，交易费还不是那么重要，因为区块奖励在矿工总收入里占比超过99%。但每4年，区块奖励就会被减半，最终区块奖励将会变得很低，低到交易费变成了矿工的主要收入来源。届时矿工会如何应对还属未知。他们会不会更加激进地要求实行最低交易费？矿工会不会联合起来逼迫比特币网络实行最低交易费制度？

未解的问题

总结来说，理论上矿工可以自由地选择挖矿的策略，但在实际中我们观察到的是大部分矿工都选择了默认策略来挖矿，虽然没有完整的模型可以证明默认策略(default strategy)就是最佳的。在本章中，我们讨论过几个特定案例，有大量算力的矿工有可能执行非默认策略来获取更大的收益。在挖矿策略上，实践是领先于理论的。在实践中，大多数矿工还是选择了默认策略，而且比特币运行得也很好。但是，从理论上，我

们还无法论证这是一个稳定的机制。

默认策略能否在实际运行中一直保持有效，对于这一点我们也没有把握。比特币运行所依赖的现实条件也一直在改变。矿工们变得越来越中心化和专业化，整个系统的算力也越来越大。另外，从长期来看，比特币的奖励将从固定的挖矿奖励为主转变为交易费为主。我们真的不知道这将会如何演变，基于博弈理论对此进行预测也是一个非常有趣的前沿研究领域。

延伸阅读

关于挖矿硬件演变的一篇优秀论文：

Taylor, Michael Bedford. “Bitcoin and the Age of Bespoke Silicon.” In Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems .Washington,DC: IEEE Press, 2013.

关于比特币和加密货币的知识系统化文章，特别是第三部分关于稳定性：

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W.Felten. “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.” Presented at the 2015 IEEE Symposium on Security and Privacy, San Jase,CA,May 2015.

一份完整的分析2011年不同矿池激励机制的文章（有些信息有点过时，但是整体上还是值得参考）：

Rosenfeld, Meni. “Analysis of Bitcoin Pooled Mining Reward Systems.”arXiv preprint arXiv:1112.4980(2011).

几篇研究挖矿策略的论文：

Eyal, Ittay, and Emin Gün Sirer. “Majority Is Not Enough: Bitcoin Mining Is Vulnerable,” In Financial Cryptography and Data Security . Berlin and Heidelberg:Springer, 2014.

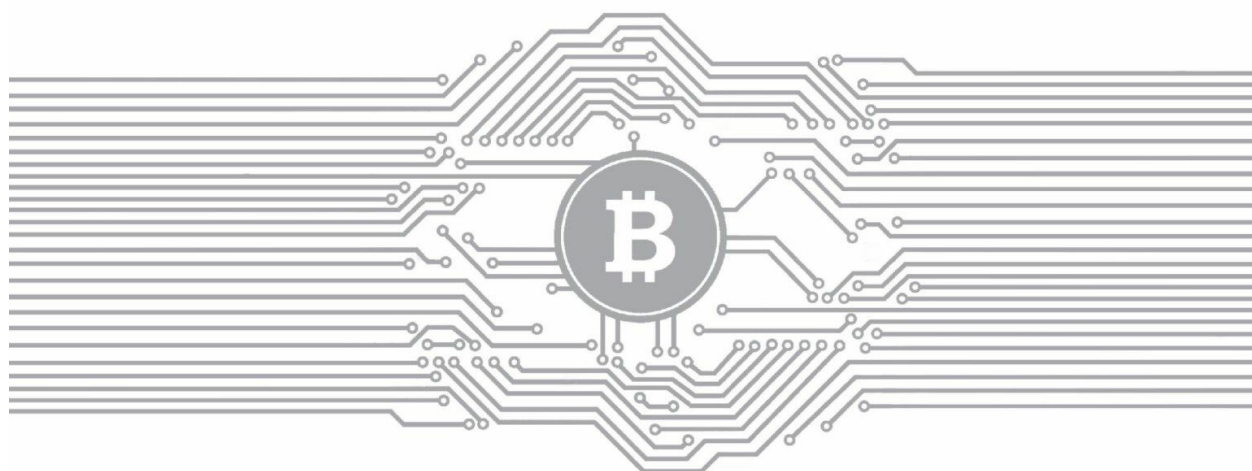
Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries.” In Proceedings of the Workshop on the Economics of Information Security 2013. Berlin:Springer-Verlag,2013.

Eyal, Ittay. “The Miner's Dilemma.” Presented at the 2015 IEEE Symposium on Security and Privacy, San Jose,CH,May 2015.

[\[1\]](#) 给自己留条后路，见机行事。——译者注

第6章

比特币和匿名性



比特币是一种安全并且匿名的数字货币。

——维基解密捐款页面

比特币并不会帮你躲避国家安全局的窥探。

——英国有线

比特币最有争议性的一个特性，就是匿名性。首先，比特币是匿名的吗？从上述两种完全相反的论调可以看到，人们对比特币匿名性存在理解上的困惑。其次，我们需要**加密数字货币**（crypto-currency）做到完全匿名吗？匿名性有好的地方，也有不好的地方，进而引申出一些基本的问题：加密数字货币的匿名性对持有者有益处吗？对社会有没有好处呢？有没有一种方法，可以让匿名性只发挥积极正面的作用，而不用担心它的负面作用呢？

这些问题很难回答，因为它们取决于人的道德价值观。本章中，我们并不会回答这些问题，即使我们仍然会探讨匿名性的优劣。我们将主要研究探讨各种技术特性，其中有一些已经是比特币所具备的，还有一些是为增强比特币的匿名性，而建议比特币应该添加的技术特性。我们也会对其他一些具备不同匿名技术特性的加密数字货币进行研究。这些技术也会带来新的问题，比如它们能在比特币或者其他加密数字货币中正常工作吗？接受这些特性有多困难？接受这些特性需要对现有的技术功能做出哪些取舍？

6.1 匿名的基础知识

匿名的定义

在讨论比特币是否具备匿名性之前，我们需要对匿名做一个定义。我们需要准确地理解到底什么是匿名，以及它与其他一些相似术语的关系，比如隐私。



匿名和化名（pseudonymity）

在其他你可能更熟悉的情形下，说明匿名和单纯的化名的区别可能更容易。其中一个很好的例子就是在线论坛，在一个类似于红迪（Reddit，美社交新闻网站）的论坛中，你会选择一个自己常用的化名在一段时间内和系统进行交互。你也可以创建多个化名，甚至每一条评论都用一个新的名字，但那样会很麻烦，绝大多数人都不会这样做。所以在红迪这样的论坛里，用户通常都会使用化名，但又不是完全匿名。相反，在4Chan（综合型讨论区）这种在线论坛里，用户通常用匿名来发帖，并且不带有任何标识性属性。

从字面上理解，匿名的意思是“没有名字”。当我们尝试用这个定义来说明比特币的匿名特征时，会有两种不同的诠释：在交易的时候不使用真实的姓名，或者在交易的时候完全不使用任何名字。比特币是否具备匿名性，这两种释义会带来两种完全不同的结论。比特币的地址是**公钥哈希值**（hashes of publickeys），在与比特币系统交互过程中，

使用者不需要使用真实的姓名，但是需要使用公钥哈希值来作为交易标识。因此，按照第一种对匿名的释义，比特币是具有匿名性的，因为使用者不需要使用真实的姓名。然而，如果根据第二种释义，比特币并不具备匿名性，因为交易中必须使用的地址是一种虚假标识。在计算机科学语言中，这种不用真实姓名而使用一种特定标识的折中做法被称为化名。

你可以根据你的需要，随意创建出任意多个比特币地址，考虑到这一点，你可能会思考比特币的地址是否真的是虚假标识，因为你可以创建无穷多的化名，正如我们将会看到的，这并不能让比特币具备匿名性。

在计算机科学中，匿名指的是具有无关联性（unlinkability）的化名，无关联性是一种针对特定攻击者的能力而定义的属性，从直观的意思看，无关联性意味着如果一个用户和系统重复进行交互，从特定攻击者的角度考虑，不同的交互行为之间应该无法互相关联。

比特币是具备化名性的，但如果你的目的是要求绝对隐私，那么这种匿名性还不够。区块链技术是一种公开的账本系统，任何人都可以查询包含了给定地址的所有比特币交易。如果有人可以用你的比特币地址链接到你的真实身份，那么所有你的比特币交易记录——不管是过去的、现在的，还是未来的——都能关联到你的真实身份。

更加糟糕的是，把比特币地址和真实身份链接起来并不困难。如果你跟某一种比特币业务有关联——不管是一个在线电子钱包服务，还是其他接受比特币的商家或交易所，通常你都需要提供你的真实身份以完成相关交易。比如，交易中通常都需要你提供信用卡信息，或者商家需要你提供真实地址以便送货上门。

或者你去咖啡馆喝杯咖啡，然后用比特币来支付。由于你已经出现在店铺里，咖啡师对你的身份特征已经有了非常多的了解，即使他们没

问你的真实姓名。你的物理标识就这样和你的某个比特币交易联系到了一起，从而可以由这个地址追踪到你所有的其他比特币交易。这显然不具备匿名性。

旁路攻击（side channels）

即使没有发生直接的关联，因为侧面渠道或者一些间接的信息泄露，你的匿名身份也可能被**暴露**（deanonymized）。举个例子，某个人看过一个匿名的比特币交易记录，并且注意到了这个比特币交易的活跃时间，那么他就可以将这个时间信息与其他公开可获得的信息关联到一起。可能他会注意到在同一个时间某一个推特用户也出于活跃状态，那么就可以建立一个匿名的比特币资料和一个真实世界的用户（至少是一个推特账号）之间的关联。很显然，这样的匿名性并不能保障隐私或者绝对匿名。要想做到绝对匿名，我们需要更强的无关联性属性。

无关联性

为了更扎实地理解比特币范畴中的无关联性特征，我们可以列举一些在比特币交易中无关联性所需要的关键属性：

1. 同一个用户的不同地址应该不易关联。
2. 同一个用户的不同交易应该不易关联。
3. 一个交易的交易双方应该不易关联。

上述第一条和第二条很容易理解，但第三条比较微妙。如果你把一笔“支付”诠释成一个比特币交易，那么第三条属性很明显就是一个伪命

题。每一笔交易都有输入和输出，这些输入和输出都不可避免地会记录在区块链网络中，并且公开地关联在一起。然而，我们所指的支付并不仅仅是一笔比特币交易，而是指任何一种从发送者到接收者的传输比特币的行为，这种行为可能会涉及一系列的间接迂回交易。我们需要确保，通过查询区块链上的信息将发送者和最终的接收者关联在一起，是不可行的。

匿名集

即使我们对支付做出更加宽泛的定义，第三条属性看起来也比较难以实现。比如说，你支付一定数量的比特币来购买某个商品，并且通过迂回曲折的形式发送了这些比特币，其他人通过查看区块链上的信息，还是可以推断出某个比特币地址上减少了一定数量的比特币，而另外一个地址上增加了差不多相同数量的比特币（可能会扣除相应的交易费用）。此外，尽管传输是通过迂回曲折的路径，初始发送方发送比特币和最终接收方接受比特币基本上发生在同一个时间段，因为商家不太愿意接受延迟付款。

基于这样的困难，我们通常并不试图在系统中，对所有可能的交易或者地址都实现完全的无关联性，而是去实现更有限度的无关联性。想象一个特定的攻击者的情况，你的交易匿名集（anonymity set）是指该攻击者无法把你的交易从其中分辨出来的交易集合。即使该攻击者知道你完成了一个交易，但是他也仅仅知道这个交易是某一个合集中中的一个，但并不能确定是哪一个。我们只需要努力去最大化这个匿名合集就可以了——在这个合集中，我们可以隐藏我们的地址或交易。

统计匿名集是很微妙的，由于这样的匿名集是针对某一个或者一组攻击者而定义的，所以你首先需要具体定义你的对手模型是怎样的。你必须仔细思考对手已知和未知的内容，以及我们需要隐藏的内容——

也就是说，如果要达到匿名性目标，交易中的那些信息是不能被对手知道的。没有成熟的公式告诉你该怎么做，需要根据每一个具体情况仔细分析相对应的协议和系统。

污点分析（taint analysis）

在比特币社区中，人们通常根据直觉推断匿名性，而非严格的定义。污点分析就是一种非常流行的方式：这是一种推算两个地址相关性的方法。如果地址S发送出的比特币总是地址R接收，那么不管是直接抵达，还是经过了多少中间地址，S和R则被定义为具有高分污点。污点分析的计算公式，适用于多个输入和（或）输出的交易，并且确定如何分配污点的规则。

遗憾的是，污点分析也不是一个衡量比特币匿名性的好方法。它只是简单地认定对手在使用相同的计算方式在关联成对的地址。稍微聪明一点的手会使用不同的技巧，比如查询交易时间，或者本章后面我们会讲的利用钱包软件的特性。所以，污点分析可能只会显示你在某种特定情况下具备的匿名性，而事实上可能并不准确。

为什么需要匿名性

了解了匿名性意味着什么之后，在我们进入更深入的探讨之前，让我们来回答一下有关匿名性的根本问题：为什么人们需要匿名性？拥有匿名性的货币有哪些伦理道德方面的意义？

在区块链货币中，所有交易都被记录在一个公共账本上，也就是说，这些记录都是公开的，并且可根据相关地址进行永久追踪，因此，你的比特币交易的隐私保护可能会比传统的银行更糟糕。如果你的真实

身份被关联到一个比特币地址，那么你就完全失去了所有交易的隐私——不管是过去的、现在的，还是未来的——只要是和这个地址相关联的交易。由于区块链是公开可用的，确切地说，任何人都有可能在你不知道的情况下识别你的身份。

考虑到这一点，我们可以认定两种不同的需要匿名加密数字货币的动机：第一种是，达到我们习惯的传统银行给我们的隐私保护级别，降低公共区块链所带来的信息暴露风险；第二种是，要超越传统银行给我们的隐私保护级别，进一步开发数字货币，使其从技术上实现任何人不能轻易追踪参与者。

匿名性的道德问题

我们有很多非常重要的理由（虽然经常被忽视）需要匿名性，传统货币已经让我们对这种匿名性习以为常。大多数人都不愿意与朋友以及同事分享他们的工资收入状况，如果你的工资是用区块链比特币支付的，而且该区块链上的地址很容易被识别，那么我们只需要关注每个月定期的大额支付记录，就能很容易地推断出你的工资情况。企业组织也有非常重要的财务隐私顾虑，例如，一家电玩游戏生产商被发现在区块链上支付给了一个分包商，而这个分包商是专门生产虚拟现实眼镜的，那也意味着它们要推出的新游戏可能会被公众（也包括其竞争对手）提前知晓。

然而，真正合理的顾虑是，匿名加密数字货币可以被用作洗钱或者从事其他非法活动。即使加密数字货币的交易本身可能是匿名的，数字货币和法定货币之间的接口却无法做到匿名，这可以说是一个好消息。事实上，我们将在下一个章节讨论中看到，这些数字货币和法定货币之间的兑换和流动被严格监管着。因此加密数字货币也不是洗钱或者其他金融犯罪的灵丹妙药。

然后有人可能会问：我们是否可以设计出一种技术，这种技术只允许使用好的匿名，而禁止坏的匿名呢？事实上，计算机安全和隐私方面的研究者一直在探索这个问题的答案，遗憾的是，从来就没有可行的方案，因为我们用道德标准分辨出的好坏，对计算机技术来说，是没有办法区分的。在比特币系统中，如何让矿工按照道德标准去判定哪些交易应该被发布到区块链中，目前还是无法实现的。

我们的观点是，启用匿名加密数字货币是有潜在好处的，这也是其得以存在的原因，同时，对于系统的技术匿名属性和在使用货币时应该遵守的法律规范，我们应该加以区分。匿名加密数字货币并不是一个完美的解决方案，但可能是最优的一种折中方案。

匿名化和去中心化

在本章中，我们会看到很多次有关匿名化和去中心化的讨论，通常这两点是相互矛盾甚至冲突的。回忆一下前言部分提到过的乔姆

（Chaum）的电子现金系统，它在一定意义上实现了完美的匿名性，不过必须依赖一个中央权威机构——银行的盲签名协议。设想一下，这样的协议的去中心化将会非常困难。如果我们强制进行去中心化，就必须要有有一种能够追踪交易并且防止双重支出的机制。交易的这种公开追踪特性，就是对匿名化的一种威胁。



Tor^[1]

如何处理一个有好坏两面性的技术，比特币并不是唯一一个面临这种道德上两难选择问题的技术。另外一个匿名性设定有争议的系统是Tor，一个匿名通信网络。

一方面，Tor的用户只是一些普通人，想保护他们在网络上不被跟踪。其用户包括记者、社会活动家和持不同政见者等，他们追求在互联网上的言论自由而不用担心政治迫害。同时，执法部门的探员也使用这个系统，监控在线嫌疑犯，而不会泄露他们的IP地址（毕竟，大家都知道IP地址是根据不同的组织机构来分配的，包括执法部门）。很显然，Tor有很多应用场景是我们从道德上认可的。另一方面，它也还有一些不好的应用场景：有人用其运作僵尸网络来控制一些被感染的电脑，进而用来传播淫秽等非法图片。

要想从技术角度去区分这些使用场景，基本上是不可能的。Tor的开发者以及社区一直在尝试解决这个难题，全社会也在努力尝试。我们似乎可以总结一下，整体而言，这样的技术利大于弊，实际上，Tor主要的投资方之一就是美国政府，其投资兴趣在于，Tor可以让不同政见者在互联网上发表自由言论，而不用担心政治迫害。同时，执法部门也勉强接受Tor的存在，甚至还开发了使用这个平台的方法。FBI也经常会查封一些在“黑暗网络”上非法传播色情图片的网站，即使这些网站也使用了Tor的平台，多数情况是，这些网站的运营者被绳之以法。我们必须记住，技术仅仅是工具，而那些犯罪分子生活在现实世界里，并可能留下各种犯罪证据，或者在使用这些工具的时候犯一些人为错误。

在本章6.5节中，我们会探讨零币（Zerocoin）和零钞（Zerocash），这是一种匿名化并且去中心化的加密数字货币系统，有点类似于乔姆的电子货币（ecash），但是因为上述两个限制，它们需要找到合适的方法，以解决棘手的加密问题。

[1] The Onion Router，洋葱路由，用户通过Tor可以在互联网上进行匿名交流。——译者注

6.2 如何对比特币去匿名化

我们已经强调过很多次比特币仅仅是一个化名系统，所以你所有的交易记录或者交易地址很有可能被关联在一起。让我们再进一步讨论这种关联是怎么发生的。

图6.1展示了维基解密的捐款页面上的一个片段（包括本章开头的时候就引用的一段），请注意那个在比特币地址旁边的刷新按钮。可能你会期望通过点击这个刷新按钮，就会把接收捐款的地址换成一个全新生成的地址。类似地，如果你刷新页面或者关闭这个页面，重新再打开的时候，这个地址也会重新生成，而且是之前没有出现过的。这是因为，维基解密需要保证每接收一笔新的捐款，都会对应一个新创设的仅用于此笔捐款的公钥。维基解密这么做就是最大限度地利用了可以创建新化名功能的作用。这事实上就是比特币钱包实现匿名性的最好途径。

比特币是一个安全的匿名数字货币系统，不容易被追踪，并且是一种有别于其他捐款方式的、更加安全和快速的方法。你可以发送比特币到以下地址进行捐款：

13DFamCvSxG8EG16VyXzdpfqxyooifswYx 

图6.1 维基解密的捐款页面的一个片段

注：请注意那个在比特币地址旁边的刷新按钮。维基解密遵循了为每一笔捐款生成一个新接收地址的比特币匿名化的最佳实践。

你可能觉得这些不同的地址一定是无法关联的，维基解密收到的不同的捐款是完全分开的，并且推测它们可以分开使用每一笔捐款，但事实并非如此。

关联性（linking）

假设爱丽丝想要去买一个茶壶，价格是8个比特币（可能根据2015年的比特币价格，实际情况应该是8分比特币，1个=100分）。进一步假设，她的比特币分在三个不同的地址里面，分别有3、5和6个比特币。实际上，爱丽丝没有一个比特币地址有足够的8个比特币，她必须要把两个输出合并成一个单体输入，以支付给店铺。



隐形地址

假设鲍勃要通过他的网站还有广告牌来宣传他的捐赠地址。现在还没有任何方式可以将一个不同的地址显示给每个用户，必然地，接收现场捐款的这个地址会很容易连接到鲍勃的站点。

能够利索地解决这个问题的办法，是利用隐形地址（stealth addresses）。它允许收件人鲍勃发布一个静态“永久”的地址，任何发件人（比如爱丽丝）由此可以派生出新的地址，该地址的私钥只有鲍勃知道。

这是如何做到的呢？回忆一下椭圆曲线数字签名算法（ECDSA）中的公钥的函数形式是 g_x ，其中的 x 是私钥，地址函数是 $H(g_x)$ 。为了启用隐形地址，鲍勃需要广告公钥本身，而不是长度更短的哈希值。然后，爱丽丝可以选取一个随机数值 r ，计算 $(g_x)r = g_{xr}$ ，并且将钱汇给这个公钥。如果爱丽丝能够单独将数值 r 发送给鲍勃，鲍勃就可以计算出正确的私钥 xr ，将汇到公钥 g_{xr} 的钱花掉。

这种方法并不完美，因为爱丽丝需要将数值 r 发送给鲍勃，而且还假定即使鲍勃不在线，比特币交易照样运行。为了解决这个问

题，还有更复杂的协议，让爱丽丝能够有效地将数值 r 嵌入比特币交易本身。随后，鲍勃可以扫描区块链，检测针对他的交易，并恢复私钥。黑暗钱包中使用了这种方法，该钱包设计时旨在增强隐私，并且类似的想法在加密签名（CryptoNote）这种另类币中有所使用。

那么问题来了，这笔交易会在区块链网络里有一个永久的记录，任何看到这个记录的人都可以推断，这两个输入型交易很有可能是由同一个用户控制的。换句话说，共享型消费，成为不同输入地址联合控制的证据。当然也可能存在例外，有可能爱丽丝和鲍勃是同寝室的朋友，决定一起联合购买这个茶壶，并且分开付款。但是，大体来说，共同输入基本上意味着共同控制。

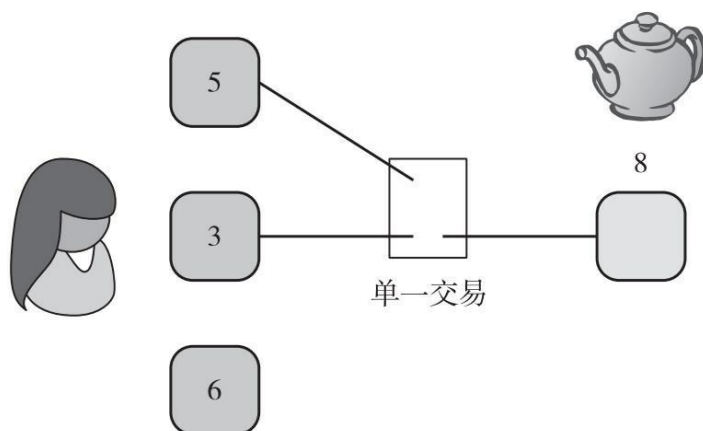


图6.2 多地址输入交易

注：为了支付购买茶壶的钱，爱丽丝从两个不同的比特币地址创建了一个单一交易。这样爱丽丝就暴露了一个事实，即一个个体控制了两个不同的地址。

还不仅仅如此，攻击者可以重复上述过程，从而一步一步将这个个体所进行的所有交易关联起来。如果另外一个地址也关联到了爱丽丝用于交易的两个地址之一，那我们就知道所有三个地址都属于同一个个体，我们可以因此建立一个**地址簇**(clustering of addresses)。一般来说，如果一个新地址的输出，和该地址簇中的任何一个已知地址被一起

花费，那么这个新的地址也将会被加到该地址簇中去。

在本章6.4节，我们将会探讨一种叫合币（CoinJoin）的匿名技术，该技术的工作原理打破了上述设想。但是到目前为止，对没有使用特别匿名技术的普通比特币钱包用户，这种簇技术还是非常有效的。接下来，我们很快将会讨论如何把这种地址簇关联到现实世界的身份。



零钱地址(change address)的随机化

早期版本的比特币类库[Bitcoin-Qt library，现在又称为比特币中心（Bitcoin Core）]存在一个缺陷，对有两个输出地址的交易，它总把存放零钱的输出地址放在第一个，这意味着很容易分辨出很多交易中的零钱地址。这个缺陷在2012年得到了修复，但是重点在于：钱包软件在保护匿名性中扮演着非常重要的角色，如果你正在开发钱包软件，你需要格外注意很多陷阱，尤其是你需要保证零钱地址的位置应该永远是随机的，以避免为攻击者留下太多信息。

再回头看一下我们的例子。假设这个茶壶的价格从8个比特币上涨到了8.5个比特币，爱丽丝发现，未用完的支出账号里无法再组合生成恰好可以支付这个茶壶所需要的金额了。取而代之的方案是，爱丽丝利用交易可以有多重支出的特性，如图6.3所示，支出的其中之一就是茶壶店铺的接收地址，而另外一个则是爱丽丝自己的“找零”地址。

现在从其他人的视角来看这笔交易，他们可以推断出这两个输入地址都属于同一个用户，他们甚至可能怀疑其中一个支出地址也属于这个用户，但是无法知道具体是哪一个。事实上0.5个比特币虽然比其他的支出小，但是并不意味着这是一个零钱地址，爱丽丝可能有10 000个比特币参与了交易，其中她支付了8.5个比特币用于购买茶壶，而把剩余

的9 991.5个比特币找零退回给了自己。在这样的场景中，更大的输出才是实际上的找零地址。

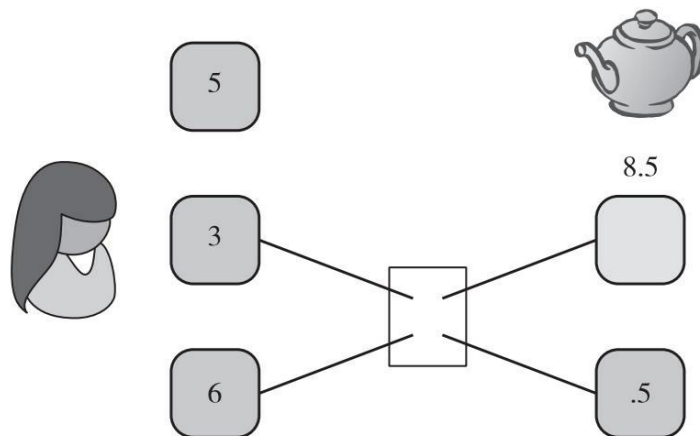


图6.3 零钱地址

注：为了支付购买茶壶的钱，爱丽丝创建了一个交易，这个交易中的一部分比特币去了商家的钱包，而剩余的部分作为零钱退回给了她自己。

另外一种更好的解释是，如果茶壶只需要花费0.5个比特币，由于不管是3个比特币还是6个比特币的输入地址，都足够用来支付了，爱丽丝根本不需要创建两个不同输入组成的交易。但是，选择哪种交易方式完全取决于通常使用的钱包软件的特性，即使不是非常有必要，钱包（或者是用户）还是可以随意组合不同交易地址中的比特币来完成支付的。

惯用法则

这种类型的实施细节被称为“惯用法则”(idioms of use)。2013年，一组研究人员发现了大多数钱包软件都在使用的惯用法则，并推导出一种用来鉴定零钱地址的强大方法。具体而言，钱包在有需要的时候都会生成一个全新的地址，因为这种惯用法则的使用，这些新的地址通常都是从来没有在区块链网络出现过的。换句话说，非零钱地址通常都不是新

地址，而是已经在区块链网络里出现过的，那么其他人就可以利用这个特性去分辨零钱地址，并把它和输入地址相关联。

依赖惯用法则来推测零钱地址可能会出错。事实上，零钱地址是新地址这一特性不过恰巧是钱包软件的一个特性。在2013年研究者测试的时候发现确实是这样，现在可能还是，但也有可能不再如此了。用户可以选择覆盖掉原来的默认设定，最重要的是，当对手了解了这种技术的时候就可以很容易回避，即使是在2013年，研究者也发现这种特征也会经常产生误报，按照这种规则可以归到一个簇的地址，不一定是属于同一个个体的。研究者声称，他们需要大量的人工监督和干预才能去除这些误报。

关联真实世界的身份到地址簇

在图6.4中，我们可以看到，米克尔·约翰（Meikle John）等人是如何利用惯用法则这样的启发式算法来聚类比特币地址的，但是这种簇没有标签——也就是说，我们还没有关联一个真实的身份到这个簇。



图6.4 地址簇

注：摘自2013年的一篇论文“一把比特币：寻找支付特征”。在一组没有姓名的用户中，研究者将联合支付的地址和全新的零钱地址归类到一个比特币地址簇。图中，圆形的大小表示流入这些地址簇里的货币数量，每一条线则代表一个交易。

我们可以根据所了解的比特币经济情况来做一个合理的推测。回到2013年，门头沟公司曾经是最大的比特币交易所，所以我们可以猜测图中较大的圆圈代表的就是该交易所控制的地址，我们可能也注意到，图中左侧的深色的圆圈代表了很小的比特币总量，但同时又有非常大的交易量，这个特性很符合叫作中本聪之骰（Satoshi Dice）的在线比特币博彩游戏，这个游戏中，你可以发送微小量的比特币作为赌注。总的来说，这并不是一个很好的方法来辨识地址簇，这需要很多背景知识和推测，可能仅仅对特征比较显著的案例有效。

利用交易进行标记

如果仅仅是通过访问交易所或者商家的网站，以查询其公布的接收比特币的地址，会怎么样呢？这其实没有实际意义。因为大多数服务提供商都会针对每一个交易公布一个新的地址，而这个新地址还没有公布在区块链网络上，等待这些地址发生交易没有意义，因为这些地址通常不会再显示给其他人。

唯一可靠的推断地址的方法，是通过和这些服务提供商发生一个实际的交易，交存比特币或者购买一个商品等。当你发送或者接收比特币的时候，你将会知道它们所拥有的地址之一，而且很快这个地址就会在区块链网络上公示（并且是在其中一个簇中的）。于是你可以为这个簇打上该服务商的身份标识标签。

这就是当时“一把比特币”的研究者（以及自那之后的其他人）追踪地址的做法，他们购买了不同的东西，加入了矿池，使用比特币交易所、钱包服务、博彩网站，以及其他一些和这些服务提供商产生比特币交易的行为，总计进行了344笔交易。

在图6.5中，我们又一次看到了图6.4的簇，只不过这一次贴上了附加的标签，我们有关门头沟公司和中本聪之骰的猜测是准确的，这些研究者同时辨识出一批其他的服务提供商，而如果不用交易的方式是很难标识它们的。

辨识个人

下一个问题是：我们是否可以对个人做同样的动作？也就是说，我们是否可以关联一些小的簇以辨识个人在真实生活中的身份？

直接交易。任何人和某个个人进行比特币交易的时候——不管是线上还是线下的商家、交易所，或者一个用比特币来分担晚餐账单的朋友——都可以通过这种直接交易，了解到他们的有效地址（至少一个）。



图6.5 标签簇

注：通过和不同的比特币服务提供商进行交易，米克尔·约翰等人得以辨识并且标记这些簇在真实世界中的身份。

通过服务提供商。在使用比特币几个月甚至几年的时间里，大多数用户都会跟交易所或者其他中心化的服务提供商有一些交集，这些服务提供商都会直接询问用户的真实身份——通常法律要求它们必须这样做。这个话题我们将会在下一个章节讨论。如果执法部门想要去辨识某一个个人，就可以直接去找这些服务提供商，要求它们提供数据。

疏忽。人们通常都会在公共论坛里公示自己的比特币地址，一个通常的原因都是通过这种办法请求捐助。当有人这么做的时候，其实已经创建了一个他们自己的身份和他们某一个地址的关联，如果他们不使用我们将要探讨的匿名服务，所有的交易都将会面临被暴露的风险。

随着时间的推移，针对隐私的攻击会变得越来越有效率。历史记录表明，当越来越多的研究者去研究并开发出新的去匿名化的技术时，越来越多的数据会被公开，去匿名化的算法也由此随着时间的推移而不断得到改进。除此之外，会有越来越多的辅助信息可以帮助攻击者去识别这些地址簇，如果你非常关心隐私，那么这个问题就值得去担忧。

目前，我们探讨的去匿名化技术，都是基于对区块链网络上交易图谱进行的分析，这些方法被归纳为**交易图谱分析**（transaction graph analysis）。

网络层的去匿名化

用户被去匿名化，有很多种不依赖于交易图谱的方法。为了在区块链网络中公示一个交易，一种典型的方法就是广播这个交易到比特币点对点的网络中，在这个网络中，消息会被相应地发送，但不一定要在区块链网络里做永久记录。

在计算机网络术语中，区块链被归为应用层，而点对点的网络则是网络层。2011年，丹·卡明斯基（Dan Kaminsky）在黑帽技术大会（Black Hat）上首次提出了网络层去匿名化的概念。他注意到，当某个节点创建一个交易时，该节点就会和其他很多节点建立链接并且广播该笔交易。如果网络上足够多的节点串通起来（或者是被同一个攻击者所控制的），他们就能分辨出第一个广播交易的节点，并且可以因此推断，这个节点就是被创建这个交易的用户所拥有的。攻击者因此可以把

这个交易关联到这个节点的IP地址，而IP地址已经非常接近于真实世界的个人身份了——有很多办法可以发现某个IP地址背后的用户身份。因此，网络层去匿名化就是隐私保护的一个非常严重的问题（参见图6.6）。

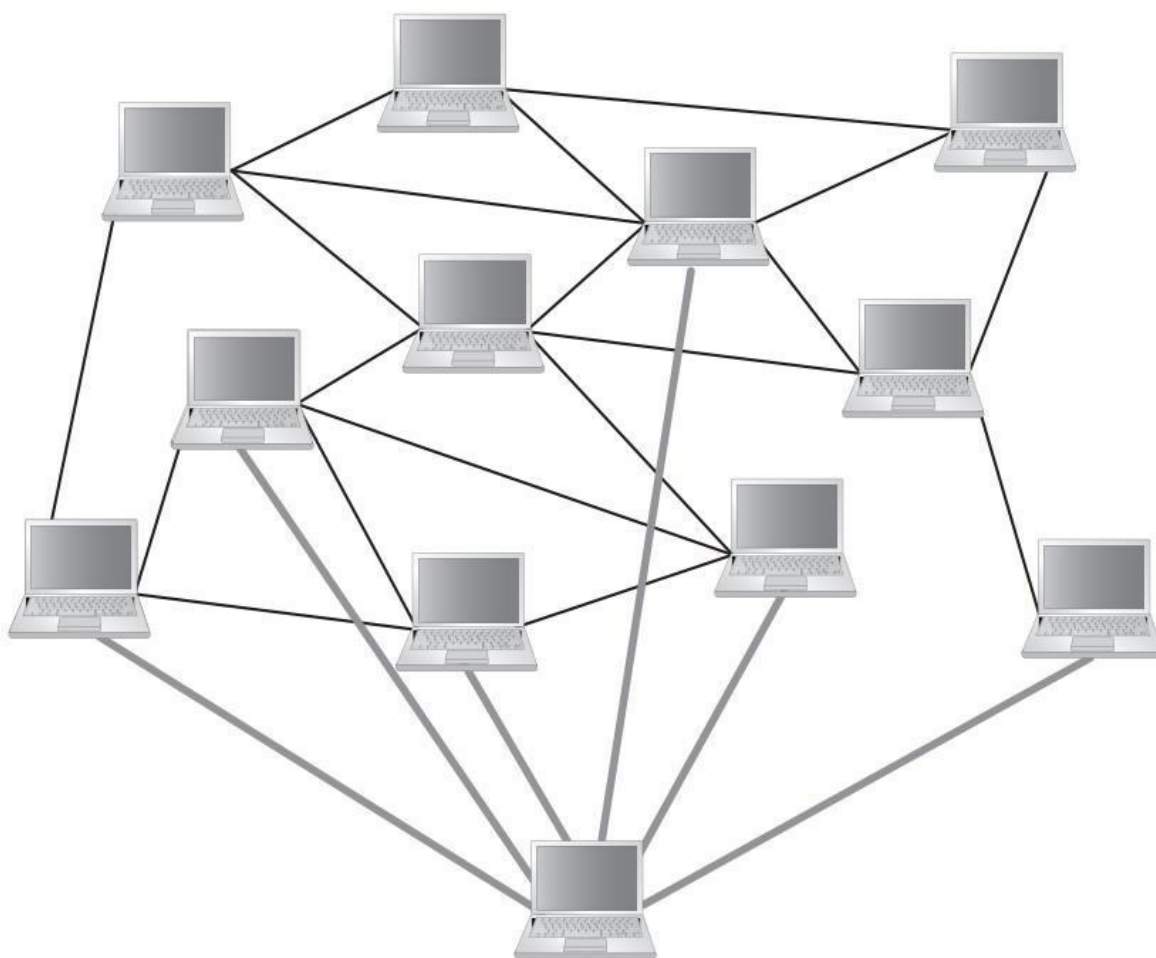


图6.6 网络层去匿名化

注：正如丹·卡明斯基在2011年黑帽技术大会上的演讲中指出的，“第一个通知交易的节点很有可能就是交易源头”。当有多个节点配合并且对同一个交易源头进行识别的时候，这种方法的实际效果会更加明显。

幸运的是，这是一个通信匿名性的问题，已经有很多研究在探索这个课题。正如我们前面在6.1节中已经看到的，Tor这个使用很广泛的系统就是用来实现通信匿名性的。

在使用Tor系统为比特币实现网络层匿名化的解决方案的时候，有几个注意事项。首先，在Tor的协议和任何基于此协议的上层协议之间，可能会有一些复杂的交互，由此可能会导致新的破坏匿名化的方法。事实上，研究者已经发现，在使用Tor协议之上的比特币时，存在一些潜在的安全问题，使用这个方案的时候一定要非常小心。其次，可能有其他一些匿名通信的技术，会更适合比特币的使用。Tor的定位是针对那些低延迟的活动，比如网页浏览。在网页浏览的时候，你也不想坐在那里等半天，因此要取得低延迟，在匿名化方面可能要做出某些牺牲。相反，比特币则是一个高延迟的系统，因为比特币交易需要花时间来获得区块链上的确认。因此，至少在理论上我们可能更希望使用另外一种替代方案来实现匿名性，比如混币网络（Mix Net，参见本章6.3节）。但就目前来说，作为一个实际在运行的并且有广大用户基础的系统，Tor还是有一些优势的，而且这些用户的安全问题已经被集中地研究过。

到目前为止，我们已经看到，通过交易图谱分析的方法，不同的地址有可能被关联在一起，甚至有可能进一步被关联到真实世界的身份。我们也看到，基于点对点网络，交易或者地址可能会被关联到一个IP地址。对后一个问题，虽然我们现在还不能说可以完全解决，但至少解决起来相对容易。前一个问题就要麻烦很多，我们将在本章的后续部分，继续探讨如何去解决它。

6.3 混币

有一些机制可以使得交易图谱分析变得不那么有效，其中一种就是混币（Mixing），这种技术背后的逻辑其实很简单：如果你想要匿名化，那就使用一个中介媒体。这个原则不是特别针对比特币的，在很多需要实现匿名性的情形下都很有用。图6.7展示的就是混币模式。

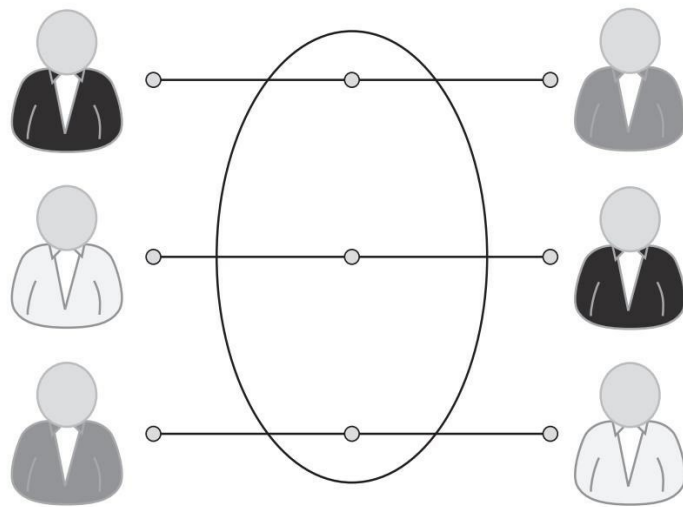


图6.7 混币模式

注：用户发送比特币给一个中介媒体，并通过其他的用户回收比特币。这就使得在区块链上追踪一个用户的比特币，变得更加困难。

混币在线钱包

如果你还记得我们有关在线钱包的讨论，那么在线钱包貌似就适合作一个交易中介。在线钱包提供了一种在线存储和提取比特币的服务，存储和提取可以在不同的时间发生。通常，你提取的比特币有别于你存储的比特币，那么，是否这就意味着，在线钱包提供了一种有效的混币服务呢？

在线钱包确实提供了一个去关联性的方法，这可以阻止交易图谱分析类型的攻击尝试，在一个具体的案例中，一些杰出的研究者不得不回撤一个面向公众的申明，因为他们之前发现的一个关联，其实只是在线钱包提供的一个伪关联。

从另外一个角度看，使用在线钱包来做混币服务，也存在一些严重的局限性。首先，大多数在线钱包并不能保证一定能实现混币功效，它们实现混币的功能，其实是因为这样做简化了开发工程。作为用户，你得不到它们不会去变更其混币模式的保证。其次，即使它们实现了混币，其内部也会保留一份记录，用来匹配你的存入和提取。这不仅是出于安全性的考虑，也是根据合规要求的审慎做法。所以说，如果你的威胁模型会考虑服务提供商本身会跟踪你，或者服务提供商被黑客攻击，又或者服务提供商被迫提供它们的记录等这些可能性，你就又回到了原点。最后，除了保留内部记录之外，声誉好的且受监管的服务提供商，也会要求你提供个人身份以进行记录（我们将在第7章中具体讨论监管问题）。你无法简单地通过一个用户名和密码，就能够创建一个账号。所以，在某种意义上，这可能比你不用钱包服务还糟糕。

在线钱包服务所提供的匿名性，和传统银行所提供的服务类似，都有一个知道所有用户的交易记录的中央媒介。对一个没有特权信息的陌生人来说，我们具备了一定程度的隐私。但是，正如我们讨论过的，区块链的公共属性意味着，如果发生任何问题（比如，钱包或者交易所服务被黑客攻击而导致内部数据的暴露），隐私风险会比传统的银行系统更大。除此之外，越来越多的人就是因为不满意传统系统的匿名性，并想要一个更好的（或者不同的）匿名性保障才转向使用比特币，这些都是用户使用专项混币服务的动力。

专项混币服务

不同于在线钱包，专门的混币服务既可以保证不留记录，又不需要你的身份验证。你甚至不需要一个用户名或者其他化名来使用这项服务，只需要发送比特币到混币服务提供的地址，并且告诉交易服务提供商你发送的比特币所需要达到的地址，混币服务提供商就会帮你转过去相同数量的比特币（不是你发送的比特币）。本质上，这是一种互换。

同时，另一个好处是这种专项混币服务承诺不会保留记录，这看上去不错。但你必须要信任它们会信守承诺，并且你还必须相信它们最终会帮你完成转账。不像在线钱包，由于混币服务并不提供一个存储比特币的地方，你需要混合后的比特币尽快回到自己手中。这也就意味着，混币池中将要和你刚刚存入的比特币混在一起的其他比特币总量会非常少，大概就是在你的比特币存入的同时其他人存入的数量。



混合（mix）和洗钱（laundry）

在这本书里，我们使用了一个术语混合，特指一个专项的混币服务，也有些人比较倾向于用另外一个同样意思的术语mixer。

你可能也遇到了洗钱这个词，我们并不喜欢这个词，因为这个词不必要地关联到了一个道德评价的问题，而实际上我们讨论的是一个纯技术的概念。正如我们所见，为什么你需要保护你在比特币运用中的隐私，并且使用混币服务来保护你的日常隐私，你有很多很好的理由。当然我们也需要了解它的负面作用，但是洗钱这样的描述加重了负面含义，因为这可能带了一种暗示，暗示你的比特币是“脏”的，需要洗干净。

还有另外一个词翻洗（tumbler），这次词的含义不是很清楚，可能会被理解为翻滚式混币的一种行为，或者是指因此而带来的清洗效果（在宝石之类的范畴）。不管怎么说，我们还是坚持使

用“mix”这样一个词。

混币准则

有一组研究者，包括本书5个作者中的4个，研究了混币模式，不仅是从增强匿名性的角度，而且还从安全信任等级方面，提出了一系列改进混币运作的方案，我们将深入探讨这些准则。

多重混币的使用

首要的原则是使用多重混币服务，一环套一环，而不是仅使用单次混币（参见图6.8）。这是一个已经被广泛接受并且已经比较完善的原则，例如，正如我们简要探讨过的Tor系统，使用了三重路由方式的匿名通信。这可以减少你对单一混币服务提供者可信赖性的依赖。只要这一系列中的任何一个混币服务提供者信守承诺并删除了记录，你就有理由相信，没有任何人能够将你的原始输入关联到你最终接收到的输出。

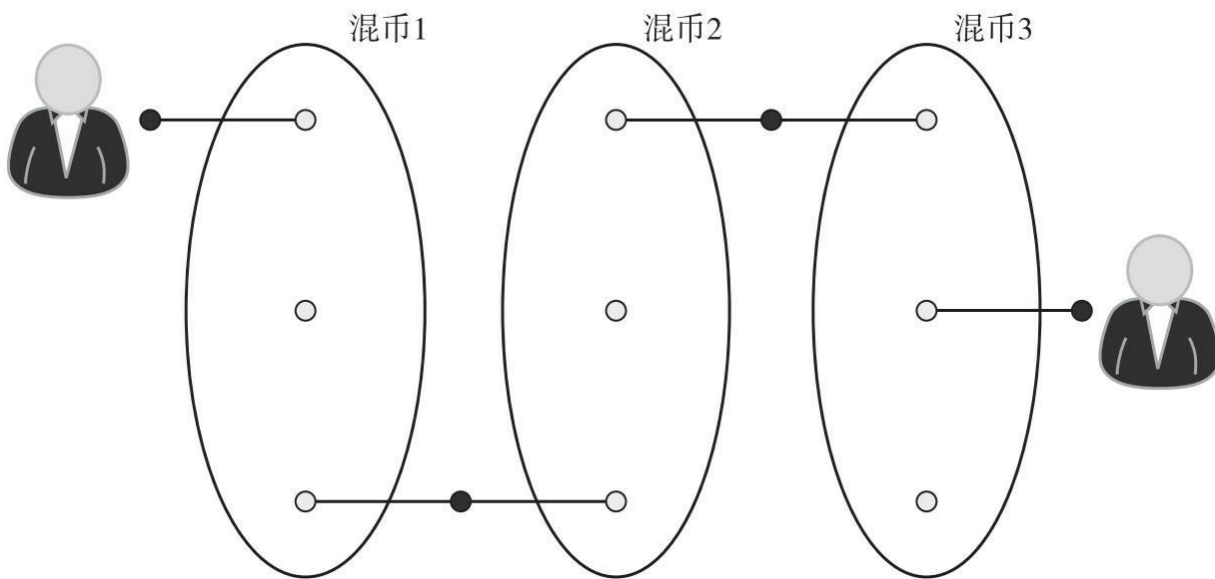


图6.8 多重混币

注：我们从一个持有比特币或者输入地址的用户开始，且假设该用户已经被其他人关联到了其具体身份。该用户通过混币服务提供商来发送比特币，每次都都需要提供一个全新产生的输出地址，只要能够在所提供的至少一个混币环节销毁输入和输出匹配的记录，而且没有其他渠道可以泄露相关信息，其他人就无法把用户最初发送的比特币和最终接收的比特币关联起来。

一致性交易（**uniform transactions**）

在混币交易中，如果不同用户使用了不同数量的比特币，这样的混币不一定会非常有效。由于初始进入和从混币过程中出来的比特币数量必须要一致，就可以通过观察某用户的比特币在混币过程中的流入流出而建立起一个关联，或者至少会极大地减少匿名集中的交易数量。

相反，我们需要混币中的交易价值能够服从平均分布，从而最小化被关联的可能性。所有的混币服务都应该对使用的块大小（**chunk size**）达成一致，也就是说，使用一个固定的混币输入值，就可以增强所有通过混币服务的交易匿名性。因为所有的交易看起来都一样，而不能通过交易价值的不同，分辨出不一样的地方。再者，在所有的混币中使用统一的大小，可以让使用多重混币更加容易，而不需要去拆分和合并其中的交易。

在实际运作中，对所有用户统一交易块大小可能会比较困难。如果我们选择的块太大，对想使用混币来处理少量比特币的用户则不适用；而如果选择的块太小，那么想处理大额交易的用户可能需要把交易拆成大量的小额交易，这种做法会非常没有效率而且成本很高。多标准块大小则可以改善性能，但是不同的块大小也会相应地分割交易匿名集。或许一系列渐增的两到三个块大小，有可能会在效率和隐私程度之间达到一种合理的平衡。

客户端自动化

除了在基于交易量的关联尝试之外，一些聪明的攻击者会尝试其他不同的方法，例如观察交易发生的时间。这些攻击其实可以防范，但必

要的预防措施对于人类来说太过复杂和麻烦。相反，混币服务的客户端功能应该是自动化的，并且是隐私保护比较好的钱包内置功能。

手续费应该是要么全有要么全无

混币服务是一种有收益期望的生意。一种计费的方式是从每一笔交易中分成，但是这种方法对匿名性的实施是有问题的，因为混币不再是统一的大小。（如果用户尝试去分拆和合并较小的交易块使得交易大小回到初始的状态，那就有可能带来严重的并且难以分析的匿名被暴露的风险，因为有更多的新的有关交易中的比特币的关联会产生。）

不要把交易手续费和混币服务费混为一谈，交易手续费是矿工所获得的，混币服务费是在此之上的额外的费用。

为了避免这个问题，混币服务费应该是要么全有要么全无，并且依概率规则来应用。换句话说，混币服务提供商应该要么在很小的概率情况下获得所有的交易金额，要么完全不收费。举例来说，如果混币服务商想要按照0.1%收费，那么应该是每1 000次交易中有一次服务提供商获得整个交易金额，而其他的999次则不收任何费用。

这个会很难实现，混币服务商需要做出一个概率决策，并且要让用户信服它们没有作弊，也就是说，在它们的随机数生成器中没有做过任何概率偏置设定。比如，获得整个交易金额的概率是1%而不是0.1%。加密学提供了一个很好的办法，你可以参考下面将要延伸阅读章节中提到的有关混币的论文，以获取更多的细节，在这篇论文中，也提到了可以让混币服务提供商提高公信力的多种其他方式。

混币实践

直至2015年，还不存在一个正常运行的混币生态系统。市场上有很多的混币服务，但是都只有比较低的交易量，因此它们的匿名组合比较小。更糟糕的是，许多混币服务提供商被报告有盗币行为，或许“自举”这样一个生态系统太难，正是混币系统从来没有良好运行过的一个原因。基于混币服务提供商狡猾的名声，并没有多少人想要使用它们的服务，这也导致了较低的交易量，进而导致了不好的匿名保护。老话说得好，大隐隐于市（anonymity loves company），也就是说，越多人使用一个匿名服务，那么这个服务能提供的匿名性就越高。进一步来说，由于提供服务并没有太多利益可图，服务提供商可能会尝试去盗取客户的资金，这会使得混币服务提供商的公信力出现持续的恶性循环。

当前，混币服务提供商并没有遵循我们所探讨的任何原则。每一个服务提供商都是独立运营的，并且通常都会提供给用户一个网页接口，让用户手工输入收钱地址和其他一些必要的参数。用户可以选择他们需要进行混币交易的数量，服务提供商针对每一笔交易收取提成来作为服务费，然后发送剩余的比特币到用户指定的目标地址。

我们认为，对混币服务提供商（和钱包软件提供商）来说，为了可以获取更强的匿名性，抵御智能攻击，提供一个高可用性的接口，进而吸引更多的交易量，实施我们介绍的模式是很有必要的。然而，迄今为止，我们还是看到过一个比较强健的混币生态系统。

6.4 分布式混币

分布式混币（Decentralized Mixing），不同于一般的混币交易，指的是用一种用户之间的点对点模式实现混币交易的协议。正如你可以想象的，这种方式在理念上与比特币更加契合。

分布式模式具有更高的可操作性。首先，分布式没有自举的问题，用户不需要等待一个有公信力的集中式混币提供商出现。其次，盗币行为在分布式混币模式下几乎不太可能发生，这种协议可以保证你可以收回你在进行混币交易时等值的比特币，正是因为这一点，即便是要进行一些对分布式混币有用的中心化的协作，由于无须说服别人自己是值得信任的，任何人都可以更加容易地设置并提供这样的服务。最后，在某些方式中，分布式混币模式可以提供更好的匿名性。

合币

分布式混币模式的主要方案被称为**合币**（Coinjoin）。在这个协议中，不同的用户共同创建一个单一的比特币交易，该交易包含所有的用户输入。让合币得以有效运作的核心技术原理为：当一个交易拥有多个来自不同地址的输入时，来自每一个输入的签名都是分离并且相互独立的，所以这些不同的地址可以被不同的人所控制，而不需要任何一方来提取所有的私钥（参见图6.9）。

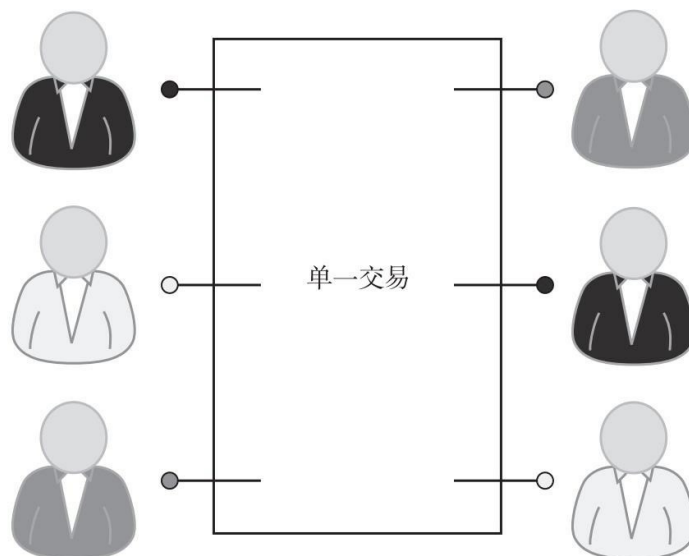


图6.9 合币交易

这样就可以让一组用户通过使用单一交易来进行混币交易。每一个用户提供一个输入和输出地址，然后组合起来就形成一个交易。由于输入和输出地址的顺序是随机的，因此攻击者无法建立输入和输出的匹配关系。参与者可以查询他们的输出地址已经包含在交易里，并且会接收到和他们输入时数量相同的比特币（减去所有的交易手续费）。一旦他们确认了这些，就可以对这个交易进行确认签名。

当其他人在区块链网络上查询这笔交易的时候，即使他们知道这是一笔合币交易，也不能确定输入地址和输出地址的匹配。从一个外来者来看，这些比特币已经被充分混币了，这就是合币的精髓。

到目前为止，我们已经描述了一轮混币交易，但是我们在6.3节中讨论的原则仍然适用，你想要（想必会）和不同组的用户重复这样的流程，你也想保证这些交易比特币块大小是标准的，这样就避免了无意中引入会造成信息泄露的旁路。

现在让我们来探究一下合币的细节，我们可以把该流程分为5个步骤：

- 1.找到想要混币的交易对手，作为节点。
- 2.交换输入 / 输出地址。
- 3.建立交易。
- 4.发送这个交易给其他人，每一个节点在确认他们的输出地址之后，进行签名。
- 5.广播这个交易。

一组想要进行混币的节点，首先需要发现彼此。这个动作需要由一个服务器来完成，其角色有点像一个“饮水坑”（watering holes）[\[1\]](#)，允许这一组用户互相连接并组合在一起。不像中心化的混币服务，这些服务器既不可能有机会盗取用户的资金，也不可能危及用户的匿名性。

一旦一组节点形成，这些节点必须要互相交换它们的输入和输出地址。地址交换中要保证即便是组中其他节点也不能知道这些输入和输出地址之间的匹配关系。这一点非常重要，否则即使你与一组看上去随机的节点进行了合币交易，攻击者还是有可能伪装自己进入这个节点组，并由此获取输入和输出的对应匹配。要做到无关联的地址交换，我们就需要一种匿名通信协议。我们可以使用之前探讨过的Tor网络，或者一种被称为加密混币网络（mix-net）的特殊目的匿名路由协议。

输入和输出地址信息一经传达，其中一个用户——不管是谁——将会基于这些相对应的输入和输出地址构建一个交易，这个未被签名过的交易将会被转发传递，每一个节点都会验证这个输入和输出地址是否正确，并且签名确认。

如果所有的节点都遵循这个协议，那么这个系统就会正常工作。任何一个节点都可以组装交易，并且任何一个节点都可以将这个交易广播到网络中，甚至这些节点中的两个可以独立广播，当然，这个交易只会

在区块链网络中被公布一次。但是，如果一个或多个节点想要进行破坏，那么启动一个拒绝服务攻击并阻止这个协议完成，是很简单的事情。

特别地，一个节点可以参与协议的第一阶段，提供输入和输出地址，但拒绝在第二阶段进行签名。或者，也可能是，在对交易进行签名确认之后，一个想要破坏交易的节点可以尝试使用它所提供给其他节点的输入地址到其他的交易中去，如果另一交易在网络中被抢先确认，那么合币交易就会被当作双重支付交易而被拒绝。

在合币交易中，有多种方案可以防止拒绝服务式攻击。其中一个就是对协议中参与交易的节点施加成本，不管是通过一种工作证明机制（类似于挖矿），或者是通过一种销毁证明机制（一种可证实能销毁你所拥有的微量比特币的技术，这一点我们在第3章探讨过）。另外的办法包括，使用一些密码学手段鉴别不符合规定的参与者，并且可以把它们从节点组里剔除。在本章结尾处，我们会看到一些相关细节。

高风险交易流（high-level flows）

我们之前谈到过旁路攻击。现在我们来仔细看一下产生旁路的玄机。我们假设，通过一个特定的地址，爱丽丝每周都固定地收到一定数量的比特币，比如43.12312个比特币，有可能这是她的薪水。进一步假设她有一个习惯，每当收到这笔资金的时候就把其中的5%立刻自动存入另外一个比特币地址，那是她的退休基金账号。我们将这种转账模式称为高风险交易流。在这种情况下，没有一种混币模式可以隐藏这两个地址之间的关系，考虑到这种行为模式会在区块链网络中是透明可见的——这样特定了金额和时间的行为，几乎不可能是偶然发生的。

有一种技术，可以帮助用户在高风险交易流的情形下重获无关联

性，这种技术叫作**合并规避**（merge avoidance），是由比特币创始人迈克·赫恩（Mike Hearn）提出的。一般来说，为了完成一笔支付，用户会尽可能地组合所拥有的比特币，以便有足够多的数额可以支付到单一接收地址来完成交易。他们是否可以规避会导致所有输入地址被关联在一起的合并行为呢？这种合并规避协议通过允许接收方提供多个输出地址的方式（尽可能多的），使得无关联性成为可能。发送方和接收方可以达成一致，通过把一个数额较大的支付分拆为一组小面值的支付方式，使得这个支付使用多个交易来完成，如图6.10所示。

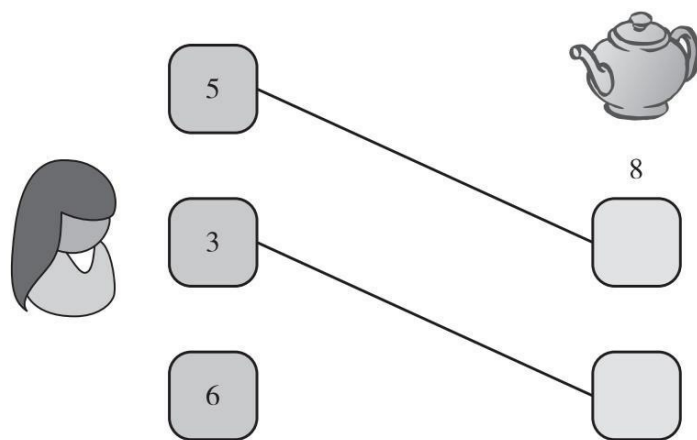


图6.10 合并规避

注：爱丽丝想要用8个比特币去购买一只茶壶，店铺提供了两个地址给她，她可以支付5个比特币到其中一个地址而支付3个比特币到另外一个地址，与她的可用输入资金匹配了，这样就可以避免暴露两个地址都是属于爱丽丝的事实。

假设，店铺最终将这两笔支付和收到的其他支付合并在了一起，这两个地址就不再是很明显互相关联的了。店铺应该避免在收款的同时，马上重新把这两个输入合并在一起，否则这两个输入来自同一个个体的事实还是会很明显。当然，爱丽丝也要避免在同一时间发送这两笔支付交易，这也有可能类似地暴露信息。

总的来说，合并规避可以帮助缓解高风险交易流的问题：如果某一个交易流水被拆分成许多互相无法关联的小额流水，攻击者可能就不会辨别这个交易。这样做也可以使依赖于识别单一交易中耗时花费的多个

比特币的地址簇技术失效。

[1] 这个比喻来自非洲草原上的饮水坑，需要饮水的动物都会到坑边去。掠食动物也常常在坑边埋伏捕猎。在网络安全上，这种类似“饮水坑”的网站也往往是黑客选择攻击目标的场所，此类攻击也被称作“水坑攻击”。

6.5 零币和零钞

在零币和零钞陆续出现之前，还没有哪个加密数字货币的匿名化方案可以让人如此兴奋，不光是因为它们所实施的密码学原理非常高妙，也因为它们承诺可以达到的匿名性非常强大有效。到目前为止，所有我们看到过的匿名加强技术，都是在原来的核心技术协议之上加载匿名化处理，零币和零钞则是在协议层就融合了匿名化处理。我们将在这里以比较大的轮廓阐述一下这个协议，并对某些细节进行了必要的简化，但读者可以在本章结尾的延伸阅读部分找到原始论文作为参考。

兼容性（compatibility）。零币和零钞为保证很强的匿名性，是有代价的：不同于中心化的混币服务和合币交易，这些协议和现在的比特币不兼容。通过软分叉（soft fork）[\[1\]](#)比特币协议的方式去实施零币在技术上是可行的，但实际操作的难度会对此造成很大的障碍。零钞甚至不能通过软分叉比特币协议的方式去实现，而只能以一种另类币（altcoin）的方式存在。

加密学保证（cryptographic guarantees）。零币和零钞在协议层已经融入了混币功能，其匿名属性来自加密学的保证，从性质上说，这些保证比我们之前讨论的其他混币技术更好。在隐私保护方面，你不需要信赖任何人，比如，混币服务提供商、混币节点，或其他任何形式的中介，甚至是矿工和共识机制协议。和大多数密码学保证一样，这种匿名性的保证仅仅依赖于攻击者的计算能力上限。

零币

为了解释零币，我们首先要介绍一下**基础币**（Basecoin）的概

念，基础币是一种类似于比特币的另类币，而零币是这种数字货币的一种延伸，其所提供的匿名性的核心特点在于，你可以将基础币和零币进行来回转换，并且当你这么做的时候，就打破了旧的基础币和新的基础币之间的关联。在系统里，基础币是你需要进行交易的货币，零币只是提供了一种交易基础币的机制，这种机制可以确保新币和旧币之间毫无关联。

你可以把你所拥有的每一个零币当作一个令牌，用来证明你拥有这么一个零币并且使其不能再被消费。这种证明机制并不会显示你所拥有的是哪一个零币，而仅仅是证明你确实拥有一个零币，稍后你可以将这个证明给矿工看，以赎回这个证明并取得一个新的基础币。用一个比喻来说，就好比你去赌场用现金换了一些扑克筹码，这些筹码就是一种证明，证明你存了多少现金，等你离开赌场时，就可以拿着这些证明去换相同数量的但并不一样的现金。当然，不像扑克筹码，除了你可以稍后用来赎回一个基础币，你并不能拿零币做任何事情。

为了在加密数字货币中让这样的机制正常运转，我们要用密码学的方式来执行这些证明，我们需要确保每一个证明只能赎回一个基础币，否则你就可以通过把一个基础币转换成一个零币，然后多次赎回获取更多的免费基础币。

零知识验证

我们使用的核心加密学工具是零知识验证，这种方式可以证明一个声明（数学上的）是正确的，而不需要展示可推导该声明正确性的任何其他信息。例如，假设你已经做了很多工作解决了一个哈希谜题，并且你想要向其他人证明你做到了。换言之，你想要证明“我做到了”这个声明。

I know x such that $H(x || \langle \text{other known inputs} \rangle) < \langle \text{target} \rangle$

当然，你可以展示上述公式里的 x 值来证明你做到了，但是零知识验证可以让你向别人证明你做到了这一点，同时不需要透露 x 的值，即便在看过你的证明之后。

你也可以证明一个如“我知道一个 x 值，而公式 $H(x)$ 的结果属于下面这一个集合 $\{...\}$ ”这样的声明。该证明既没有展示 x 值是什么，也没有证明集合里面到底哪一个元素等于 $H(x)$ 。至关重要的是，零币就是利用零知识验证来实现其功能的。事实上，零币中被这种方式证明的声明，与后面要提到的例子非常相似。本书中，我们把零知识验证当成一个黑匣子，只说明了零知识验证可以实现的属性以及在这个协议中的哪个部分是必需的，我们并没有深究如何实现这一功能的技术细节。零知识验证是现代密码学的一个基石，是很多相关技术协议的基础。再一次强调，我们建议有兴趣的读者可以参考延伸阅读中提到的文献，去了解更多更加详细的内容。

铸造零币

零币通过铸币过程而产生，而且任何人都可以铸造一个标准面值的零币。为简便起见，我们认为零币只有一种面值，每一个零币价值一个基础币。虽然任何人都可以铸造一个零币，但是产生的零币并不自动具备任何价值——你不可能获得免费的钱。只有把零币放到区块链网络上，并且通过消耗一个基础币的方式，它才能具备价值。

为了铸造一个零币，你需要使用加密学承诺。回顾一下我们在第1章讲过的内容，承诺方案类似于将一个值放入一个信封，并将信封置于所有人的视野中（见图6.11）。



图6.11 一个序列号的承诺

注：密码学承诺好比把一个序列号封装到一个信封里。

铸造零币的过程分为三步：

1.生成一个序列号 S 和一个随机密钥 r 。

2.计算一个函数 $\text{Commit}(S, r)$ ，这是序列号 S 的承诺。

3.如图6.12所示，在区块链上发布该承诺，这需要消耗一个基础币，此币不可再被花费，进而创建了一个零币。此时并 S 和 r 仍然是保密的。

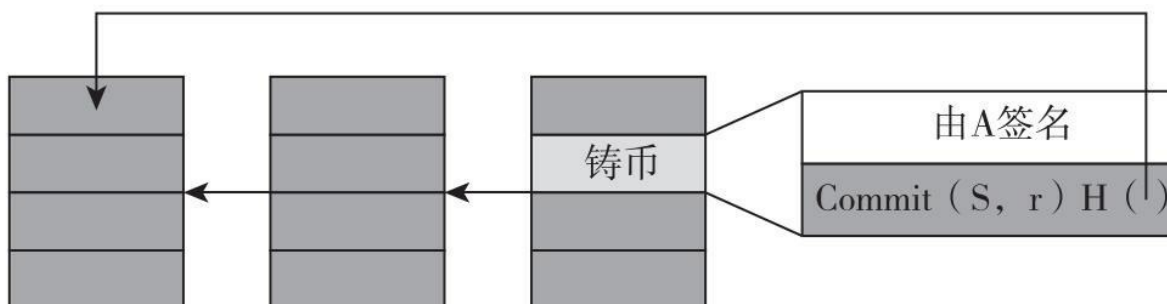


图6.12 在区块链网络上设置一个零币

注：为了将一个零币置于区块链中，需要创建一个铸币交易，其输出地址是零币序列号的一个密码承诺，而铸币交易的输入则是一个基础币，这个基础币也会在创建零币的过程被消耗掉，整个交易过程并不需要公示这个序列号。

为了消耗一个零币并赎回新的基础币，你需要证明你之前已经铸造了一个零币，你可以通过公开之前的承诺也就是说公示 S 和 r 的值来证明这一点，但是这样显然就建立了一个你的旧的基础币和新的基础币之间的关联，那么我们怎样才能打破这个关联呢？这个时候就用到零知识验证了，在任何时间节点，区块链网络上都有很多的承诺对象——我们将其命名为 c_1, c_2, \dots, c_n 。

以下是消耗一个具有序列号 S 的零币以赎回一个新基础币的步骤：

- 创建一个特殊的“花费”交易，这个交易包含序列号 S 和一个具备零知识验证的声明：“我知道在承诺对象 (S, r) 中的 r 在以下的集合里： $\{c_1, c_2, \dots, c_n\}$ ”。

- 矿工将会验证你的零知识验证，这将给予你打开区块链中一个零币承诺的能力，而你并不需要真的打开它。

- 矿工也会查询序列号 S ，确认这个零币没有在之前的花费交易中被使用过（为了防止双重消费）。

- 你的花费交易的输出将形成一个新的零币，你应使用你所拥有的一个地址来作为输出地址。

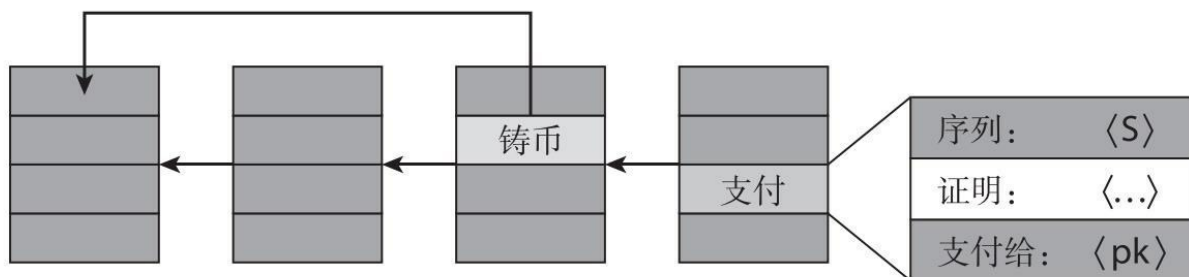


图6.13 花费一个零币

注：花费交易展示了之前铸币交易中所锁定的序列号 S ，以及 S 和之前的铸币交易的关联性的零知识验证。不像一个铸币交易（或者一个普通的比特币 / 基础币的交易），这个花费交易没有输入地址，因此也没有签名，只有一个零知识验证的证明来确立它的有效性。

一旦你花费了一个零币，其序列号就变得公开了，那么你就不能再次赎回同一个序列号所对应的零币，由于每一个零币都仅有唯一的序列号，正如我们从安全角度所要求的那样，每一个零币只能被花费一次。

匿名性。在整个过程中，我们可以发现 r 一直是保持隐匿状态，不管是铸币交易还是花费交易都没有展示过 r ，这意味着没有人知道哪一个序列号对应哪一个具体的零币，这就是零币匿名性背后的核心概念。在区块链上，生成序列号 S 的铸币交易和稍后公示 S 以赎回一个零币的花费交易之间，并没有关联性。这种听起来像魔术般的特性是无法使用实体的封装系统来实现的，但在密码学中是可以做到的。好比我们在桌上放了一些装有不同序列号的密封过的信封，你可以证明某一个序列号是这些信封里面的一个，而不需要展示是哪一个，也不需要打开任何一个信封。

效率。回忆一下我们在花费交易中证明过的一个声明：

“我知道在承诺对象 (S, r) 中的 r 在以下的集合里： $=\{c_1, c_2, \dots, c_n\}$ ”。

其中， n 代表的就是曾经被创建过的零币的数量。听起来这种零知识验证的实施会变得非常没有效率，因为证明中包含的集合大小会随着

n的增加而线性增大。神奇的是，零币可以让这种验证的复杂度仅仅是n的对数。我们需要注意到这一点，即使需要被验证的声明的长度是线性的，声明本身并不需要被包括在证明里，而是隐含的。由于矿工们知道区块链上所有零币的集合，声明就可以被矿工们自行推断出来。这样证明本身就可以非常短。尽管如此，跟比特币相比较，零币还是增加了相当大的额外开销，大概50KB。

建立信任

用于搭建零币的工具之一（RSA累加器）需要进行一次性信任设置。特别的是，一个被信任方需要选择两个大的质数p和q，并且公示 $N=p \times q$ 作为所有人在系统的整个生命周期中使用的参数。我们可以把N看作一个公钥，只不过它被用于所有的零币而不是仅仅对应于某一个体。只要这个被信任方，销毁任何关于p和q的记录，系统就可以被认为是安全的。需要强调的是，这一做法是基于对两个大质数的积进行因子分解是不可行的这一假设的普遍认可。但是，如果任何人知道了秘密的因数p和q（也被称为“陷阱门”），他们就可以在不被监测到的情形下，为自己创建新的零币。所以，这些秘密的输入只能被使用一次，在用于产生相对应的公钥后就被销毁。

这里有一个有趣的社会学问题，一个个体怎么选择这个N并能够让每个人相信，在设置时使用的相对应的质数p和q，已经被安全地销毁了，这一过程还不是很清楚。如何实现这个目标，会有很多不同的方案，其中就包括“阈值加密”技术，该技术可使用多个代理协同计算出N，而只要其中一个代理将自己的秘密输入销毁，这个系统就可以被认为是安全的。

我们还可以使用其他略有不同的加密构造来避免设置这样一个被信任方。特别是，有实践表明，随机生成一个大数就具有很高的安全性，

因为这样一个数字很有可能不能被完全分解。但遗憾的是，这样做会带来很大的效率冲击，因此这种方法并不实用。

零钞

零钞是一种不同的匿名性加密数字货币，它建立在零币的概念之上，但将加密技术提高到了更高的层次。零钞使用的是一种被称为zk-SNARKS^[2]的密码学技术，这种技术可以使得零知识验证更加简洁、更加有效率，要点就在于，系统的整体效率可以达到某一定程度，使得整个网络可以不需要依赖一种基础币而运行，所有的交易都可以以零知识验证的方式进行。如我们所看到的，零币也支持那些本不需要无关联性的普通交易，只不过在其上做了计算量昂贵的混币交易进行补充。这种混币交易由固定面值的数字币组成，交易价值的拆分与合并只能在基础币系统里实现。在零钞系统中，这种差异就不存在了，交易金额的大小被封装在一个承诺中，在区块链上不再可见，密码学证据确保了拆分与合并的正确性，用户并不能凭空创造出零钞。

账本公开记录的唯一内容就是交易的存在性，以及矿工们用来验证系统正常运行所需要的关键属性的证明。区块链网络上既不显示交易地址，也不显示交易价值。唯一需要知道交易金额的用户，是本次交易的发送方和接收方，矿工们是不需要知道的。当然，如果其中存在交易费用，矿工们则需要知道的仅仅是手续费，这点也不会影响匿名保护。

就匿名性和隐私性来说，零钞这种完全不可追踪的交易系统自成门派。因为公开账本并不包含交易金额，零钞对针对混币服务的旁路攻击是免疫的。

建立零钞系统

按照技术属性来说，零钞看起来好得有点不真实。其实它确实也有自己的命门。就像零币，零钞也需要一个“公开参数”来设置这个零知识验证系统。但是不同于只需要一个几百个字节长度的数字N的零币，零钞需要的是一个很大的公开参数集——其大小超过1G字节。要再次强调的是，为了生成这些公开参数，零钞需要一组随机并且秘密的输入。如果任何人知道了这些秘密输入，就会产生无法监测的双重消费问题，从而危及整个系统的安全性。

在这里，我们不会过多地深入探讨设置一个zk-SNARK系统所面临的挑战，这个问题也是一个比较活跃的研究方向，但是截至2015年，我们并不知道如何在实际操作中以足够稳妥的方式建立这个系统。迄今为止，zk-SNARK还没有被实际运用。

综合比较，融会贯通

现在，让我们从匿名性以及实际的可操作性两个方面，来比较以下我们所探讨的这些方案，见表6.1。

表6.1 本章所讨论的匿名技术的比较

系统	类型	对匿名性的攻击	可部署性
比特币	化名	交易图谱分析	默认系统
人工混币	混币	交易图谱分析，恶意的混币服务提供商，恶意的混币对手方	已被应用
多重混币/ 合币	混币	旁路攻击，恶意的混币服务提供商，恶意的混币对手方	兼容比特币
零币	加密混币	旁路攻击（存在可能性）	另类币，需建立信任方
零钞	不可被跟踪	未知	另类币，需建立信任方

我们是从比特币，这个已经成功部署了的“默认”系统开始的。但比特币只是化名系统，我们看到，强大的交易图谱分析是可能攻击比特币的匿名性的一种可行办法。我们也探讨了聚集大量地址簇方式，以及如何关联真实世界的身份到这些地址簇的方法。

匿名化技术的下一等级，是用人工的方式实现一个单一混币交易，或者通过人工找交易对手的方式来实现合币交易，这会使输入地址和输出地址之间的关联变得模糊，但同时也会在交易图谱中留下了太多的线索。除此之外，混币服务提供商和参与节点也可能是恶意的，或者因为被黑客攻击的，或者被胁迫公布记录的。即使从匿名性来说离完美还很遥远，但混币服务在现实中存在，并且是现今一个可用的选项。

我们讨论的第三个等级的匿名性，是混币服务链或者合币交易。这种匿名性上的改进，来自更少的对于混币服务提供商或者节点组的依赖。诸如标准化的交易区块大小和客户端的自动化等特性，可以最小化信息泄露的可能性，但是还是有一些旁路风险可能会存在。同时，也还是存在一些攻击者可能控制或者勾结多个混币服务商与参与节点而带来的风险。实现带有混币服务链功能的钱包和服务在技术上是可行的并且应该会被用户所接受，但是据我们所知，一个安全的混币链解决方案还不存在。

接下来，我们探讨了把加密技术直接应用到协议层并提供匿名化的数学保证的零币。我们认为零币的旁路攻击风险还是存在的，但是明显已经优于其他的混币解决方案。不过，零币需要作为相对于比特币的一种另类币的方式发行。

最后，我们探讨了零钞。通过效率上的改进，零钞可以作为一个完全无法追踪——不仅仅是匿名化——的加密数字货币。然而，就像零币一样，零钞和比特币并不兼容，更糟糕的是，零钞需要一个非常复杂的建立流程，数字币领域仍然在研究如何用最好的方式来实现它。

在本章中，我们讨论了很多技术。现在让我们退一步看，比特币的匿名性（或者匿名潜力）是强大的，当和其他一些技术配合的时候会更加强大，尤其是在匿名通信方面。如我们在第7章中将要讨论的，这是一些匿名在线市场所使用的强有力的技术组合方式。

尽管匿名化技术是强大的，但同时也是脆弱的。一个错误就可能造成一个我们不希望看到的，但又是不可逆的关联。匿名化有一些显而易见的有害应用，但同时也存在很多有益的应用，所以是值得保护的。虽然道德层面上的区分很重要，我们还是无法在技术层面清楚地辨识。匿名技术看起来具有深入的和固有的道德模糊性，作为人类社会的一员，我们必须学会怎么面对这个现实。

和关于比特币的道德争论一样，比特币的匿名性也是一个很活跃的技术创新领域。我们仍然不知道比特币的哪一种匿名系统，如果存在的话，将会脱颖而出成为主流。这也将是每一个人的机会——不管你是一个开发者、一个政策制定者，还是一个普通用户——每个人都可以参与其中并做出贡献，希望你在本章中里所学到的内容，可以为你提供一些正确的背景知识去采取行动。

延伸阅读

与前面几章中讨论的主题相比，匿名技术在更快地持续发展中，并且是加密数字货币研究领域中更活跃的一个课题。想要跟上这个领域中最新的进展，可以阅读以下列举的论文，以及引用其他论文。

关于交易图谱分析的《一簇比特币》：

Meiklejohn,Sarah,Marjori Pomarole,Grant Jordan,Kirill
Levchenko,Damon McCoy,Geoffrey M.Voelker,and Stefan Savage.“A
Fistful of Bitcoins:Characterizing Payments among Men with no Names.”In

Proceedings of the 2013 conference on Internet measurement, New York:ACM,2013.

关于我们讨论的混币技术和有效混币原则的来源的研究：

Bonneau,Joseph,Arvind Narayanan, Andrew Miller,Jeremy Clark,Joshua A.Kroll,and Edward W. Felten.“Mixcoin:Anonymity for Bitcoin with Accountable Mixes.”In Financial Cryptography and Data Security. Berlin:Springer,2014.

混币服务实践研究，其中很多种并没有很好的声誉：

Möser Malte,Rainer Böhme, and Dominic Breuker.“An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem.” In 2013 eCrime Researchers Summit .Washington,DC:IEEE,2013.

比特币论坛里，比特币核心开发者格雷·麦克斯韦（Greg Maxwell）发布的有关合币的内容：

Maxwell, Gregory.“CoinJoin: Bitcoin Privacy for the Real World.” Bitcoin Forum, 2013.下载地址<https://bitcointalk.org/index.php?topic=279249.0>.

来自约翰·霍普金斯大学（Johns Hopkins University）的密码学者开发了零币，请记住零币和零钞是这本书里我们讨论过的最复杂的加密技术：

Miers,Ian,Christina Garman,Matthew Green,and Aviel D.Rubin.“Zerocoin:Anonymous Distributed E-Cash from Bitcoin.”In Proceedings of the 2013 IEEE Symposium on Security and Privacy .Washington,DC:IEEE,2013.

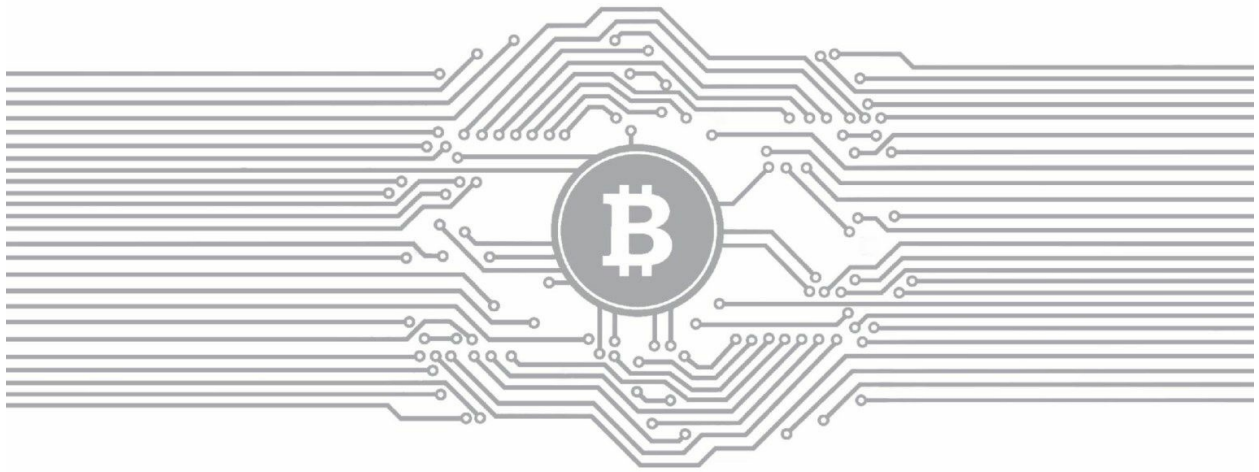
零币的作者和其他一些开发了SNARK技术的研究者共同开发了零钞系统：

Ben Sasson,Eli,Alessandro Chiesa,Christina Garman,Matthew Green,Ian Miers,Eran Tromer,and Madars Virza.“Zerocash:Decentralized Anonymous Payments from Bitcoin.”In Proceedings of the 2013 IEEE Symposium on Security and Privacy .Washington,DC:IEEE,2013.

[1] 所谓软分叉在比特币中的含义是对协议进行向前兼容的修改。修改后的新版本会造成原有的部分区块或交易无效，但是按更新后的协议产生的新交易和区块在旧协议下是有效的。换句话说，新协议是原协议的一个子集。——译者注

[2] zk-SNARK的全称是zero knowledge Succinct Non-interactive ARgument of Knowledge，是近年兴起的一种密码学方法。Snark在英文中本就有鬼魅的含义，用到这个技术上倒也有几分神似。——译者注

第7章 社区、政治和监管



在本章中，我们将研究比特币世界和数字加密货币技术是如何影响世界的，并探讨比特币社区的内部政治以及比特币是如何与传统政治，即执法和监管问题互相影响的。

7.1 关于比特币的共识

首先，让我们看一下在比特币问题上已达成的共识，它是比特币运行的基础。为使比特币顺畅运行，人们必须就以下三个问题达成共识：

1.关于规则的共识。这里所说的规则是指包括确保交易或区块有效的机制，及比特币运行时涉及的核心协议和数据格式等内容。人们需要就这些规则达成共识，这样，比特币系统中的所有参与者才能就发生的情况相互沟通并达成协议。

2.关于历史记录共识。也就是说，参与者必须对区块链的内容，包括哪些是属于区块链，哪些是不属于区块链的内容达成共识，这样，人们才能就如何确认已发生的交易达成共识。在此基础上，人们就可以对比特币、未动用产出的数额及拥有人达成共识。这一共识源自区块链的创建过程和使各个节点对区块链内容的理解达成一致的过程，我们已经在第1章和第2章中对这些过程进行了描述。这是比特币中最常用且技术上最复杂的一种共识。

3.关于比特币价值的共识。第三种共识要求人们普遍认为比特币是有价值的，比如，如果有人今天给了你一个比特币，你明天就能够将它兑现或用它换取到有价值的东西。任何一种货币，不管是像美元这样的法定货币，还是像比特币一样的数字加密货币，赖以存在的基础都是其具有价值的共识。也就是说，人们普遍接受可以用它进行交易，在现在或未来可以用它换取其他有价值的东西。

对于法定货币，第三种共识是唯一的共识。“货币有价值”这一共识不是由规则决定的，法律规定了它是不是钞票。历史记录并不重要，但是状态很重要——谁拥有什么。状态由物质占有（如持有现金）或专业记录（如银行）来决定。然而，对于数字加密货币，人们还需要对规则

和历史记录达成共识。

对于比特币，与其他共识不同的是，这第三种共识具有一定的循环性。即，我相信我今天收到的比特币是有价值的，这取决于我希望明天收到这个比特币的人同样相信它的价值。因此，对价值共识的基础在于对价值延续性的共识。这有时被称为“仙子效应”（Tinkerbell effect），这个名字来源于童话故事《彼得潘》，仙子之所以存在，是因为你相信她存在。

不论是否循环，对于价值的共识都是存在的，这对比特币系统的运行至关重要。而且，还有很重要的一点是，这三种共识相互关联，如图7.1所示。

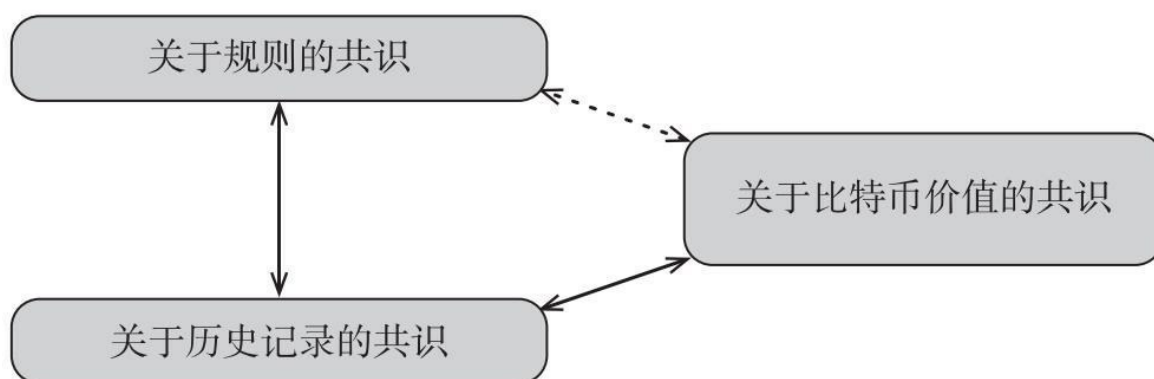


图7.1 关于比特币的三种共识之间的关系

首先，对规则与对历史记录的共识相互依赖。如果不知道哪些区块是有效的，也就无法对区块链达成共识。如果不能对区块链中有哪些区块达成共识，也就无法判断交易是否有效，进而无法判断有没有双重支付的企图。

对历史记录和对比特币价值的共识也紧密相关。对历史记录的共识意味着我们同意谁拥有哪些比特币，这是比特币具有价值的先决条件——例如我拥有一个比特币，如果不能通过历史记录对此达成共识，我就不能指望将来某一天我会把这个比特币付给某人换取其他东西。反之

亦然——在第2章我们讨论过，对比特币具有价值的共识，激励着矿工维护区块链的安全，这又促使我们对历史记录达成共识。

比特币原始设计的天才之处就在于，它意识到靠自己本身很难达成这三种共识的任何一种。在一个没有身份概念的、去中心化、全世界范围内运行的系统中，要达成关于规则的共识是不可能的。

类似地，对历史记录的共识是一个复杂的分散式数据结构问题，很难靠自己解决。此外，对某种数字加密货币具有价值的共识也很难达成。但比特币的设计以及运行模式表明，尽管无法靠系统本身达成这三种共识中的任意一种，不过可以通过某种方式将这三种共识组合在一起，并让它们以一种相互依存的方式发挥作用。因此，在讨论比特币社区的运作模式时，我们必须牢记，比特币系统的运行取决于参与者的共识，而且这种共识是十分脆弱的，交织着各种技术和社交元素。

7.2 比特币核心钱包软件

比特币核心钱包（bitcoin core）是一款开源软件，是对比特币规则进行讨论和争议的焦点。这款软件由极为宽松的开源（open source）许可证——MIT许可证认证。只要注明版权声明和许可声明，就可以将该软件用于各种用途。比特币核心钱包是目前运用最为广泛的一款比特币软件。即便不利用它进行软件开发，许多人也会通过研究它来了解比特币的规则。在构建其他比特币软件时，人们会借鉴其规则定义部分的内容，包括判定交易和区块的有效性。

比特币核心钱包实际是比特币的规则手册。通过研究比特币核心钱包及其相关解释，可以了解到在比特币系统中真正有效的内容。

比特币改进方案

任何人都可以通过“提交请求”（pull requests）按钮，帮助比特币核心钱包进行技术改进，这一过程在开源软件（open-source software）世界极为常见。若想对软件进行更大的改动，特别是对协议进行修改，则可以通过一个较为正式的叫作比特币改进方案（Bitcoin Improvement Proposal，简称BIP）的流程来实现。因此，如果你有意通过技术改变来改进比特币，你可以把你的想法写下来，根据比特币改进方案的要求，与其他文件一起公开发表。这会触发比特币社区就你的方案进行讨论，并决定下一步行动。虽然任何人都可以提交正式方案，但正如所有开源项目（open-source project）一样，这存在学习曲线。

BIP以编号序列形式发布，每项方案有一名拥护者，负责宣传方案、协调讨论活动并努力促成方案在比特币社区向前顺利开展或实施。

我们上面所说的内容适用于对技术更改的方案。事实上，也存在一些BIP，或者只是为了提供信息，传播关于比特币的知识；或者将之前仅在源代码中明确的部分代码进行标准化。而其他一些BIP侧重流程，讨论比特币社区如何决策事项。

总之，除了包含规则手册中的内容外，BIP还包含方案、制定和讨论规则变更的流程。

比特币核心钱包开发人员

要了解比特币核心钱包的作用，我们需要了解比特币核心钱包开发人员所发挥的作用。原始代码的作者是中本聪（Satoshi Nakamoto），我们在7.4节还会介绍。现在，中本聪本人已经不再活跃，但还有一群开发人员在维护着软件。有数百名开发者在为这个项目写代码，但只有少数几个人拥有对核心钱包数据库的“调配”（commit）权限。这些核心钱包的首席开发人员持续维护该软件，并决定哪些新代码可以加入软件新版本中。

这些人的权力有多大？从某种意义上说，他们的权力是很大的，因为他们对代码做出的规则改变终将呈现在比特币核心钱包中，这些规则会默认被遵守。这些人写下比特币事实上的规则手册。但从另一个角度来看，他们根本就没有什么权力。因为这是一款开源软件，任何人都可以复制、修改它（随时创建一个比特币分叉）。因此，如果首席开发人员的表现不被社区接受，社区可能走向不同的方向。

可以这么想，首席开发人员就像在引领游行队伍前进。他们在队伍的最前面，当他们拐弯时，队伍一般会跟着他们拐弯。但是如果他们试

图把队伍带入灾难性的境地，那么队伍中的其他成员可能会选择不同的方向。这些首席开发人员可以敦促社区，但是，如果他们试图把系统带入不被社区接受的技术方向，他们并没有正式的权力，来迫使人们跟随他们。

现在来思考一下，作为系统的使用者，如果你不喜欢它的规则或系统运行的方式，能够做些什么，并与集中式货币（如法定货币）进行比较。在集中式货币系统中，如果有异议，你有权退出，也就是说，你可以不用它。你必须想办法把持有的货币卖出，然后移居到使用另一种货币的地方。有了集中式货币，退出是你的唯一选择。

在比特币系统，你当然也有权退出，但是，因为它作为开源系统（open-source system）运行，你就有了对规则进行分叉的权利。也就是说，你、你的朋友和同事可以选择运行一套不同的规则，而且，通过对规则进行分叉，走向与首席开发人员不同的方向。与退出相比，分叉赋予用户更多的权力，像比特币这样开源系统的社区比完全集中系统的社区拥有更多权力。所以，虽然首席开发人员看似一个拥有控制权的集权式实体，事实上，他们并不拥有一个完全集权式管理人员或软件所有者所拥有的权力。

规则分叉

创建软件分支或规则分叉的一种方式，是以新的创世区块创建新的区块链。人们经常通过这种方式来创建另类币，我们将在第10章谈到这个问题。现在，我们来谈谈对规则的另一种分叉，这种分叉不仅对规则进行分叉，还对区块链进行分叉。

在第3章中，我们谈到了硬分叉和软分叉之间的区别，这里我们谈的是硬分叉。当对规则有分歧时，区块链中会有分叉，导致两个分支。

其中一个分支在规则A下有效，而在规则B下无效，反之亦然。矿工一旦在两种不同的规则下操作，他们就无法合并到一起，因为每个分支都将包含在另一规则下无效的交易或区块。见图7.2。

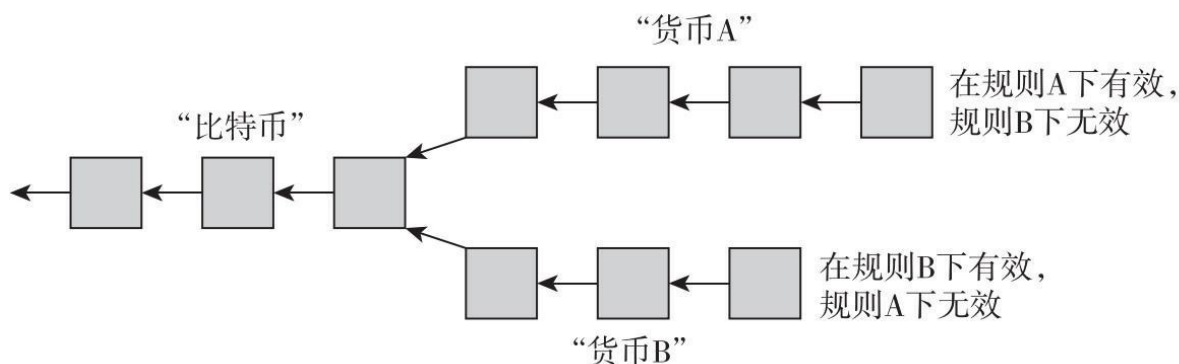


图7.2 货币中的分叉

注：如果规则的分叉导致区块链的硬分叉，那么货币本身就会分叉成两种新货币。

我们可以把分叉前的货币看作比特币，深受人们认同和喜爱的比特币。分叉之后，出现两种新货币，符合规则A的货币A和符合规则B的货币B。分叉时，每一个持有一个比特币的人得到一个货币A和一个货币B。分叉后，货币A和货币B开始分开运行，而且它们可能会独立运行。这两者的规则还可能以不同方式继续发展。

需要强调的是，不仅仅是软件，或规则，或实现规则的软件分叉了，货币本身也分叉了。这个有趣的现象只可能发生加密数字货币中，却不能发生在传统货币中，因为传统货币并不允许用户将货币进行分叉。就目前我们所了解的情况，不管是比特币还是任何另类币，尚未以这种方式分叉过，但确实存在这个奇妙的可能。

人们会对这样的分叉做出何种反应呢？这取决于分叉的原因到底是什么。第一种情况是，进行分叉的原因并不是对规则存在异议，而是想创建一种另类币。如果想创建一种与比特币规则类似的另类币，有些人会通过将比特币的区块链分叉的方式来实现。这对比特币社区来说并不构成真正的问题，另类币单独运行，与比特币主分支和平共存，一些人

偏好比特币，另一些人更偏好另类币。但是，正如之前我们说过的，截至目前，还没有人通过将比特币或现有另类币的区块链分叉的方式来创建新的另类币，他们一般都通过新的创世区块来创建。

一个有趣的情况是，如果分叉的原因是人们对比特币的未来发展存在分歧，换言之，比特币社区内部发生叛乱，因为一些成员认为自己对系统如何运行有了更好的想法，决定脱离出去。在这种情况下，两个分支成为对手，会争夺市场份额。货币A和货币B都会努力说服更多商家接受它，让更多人购买它。每种货币都想成为“真正的比特币”。它们都声称自己是合法的，并将对方描述成一个怪胎，这可能会引发一场公关之战。

结果很可能就是某一分支胜利，另一分支则渐渐消失在人们的视线中。这种类型的竞争往往指向某一方向。一旦人们认为这两个分支中的某一个更合法并获得了更大的市场份额，网络效应会越来越明显，而另一种货币将成为一种利基（niche）^[1]货币并将最终消失。获胜方的规则和管理架构将成为比特币事实上的规则和管理架构。

^[1]（商业用语）是指针对企业的优势细分出来的市场，这个市场不大，而且没有得到令人满意的服务。产品推进这个市场，有盈利的基础。在这里特指针对性、专业性很强的货币。
——译者注

7.3 利益相关者：谁是掌权者

比特币的利益相关者有哪些？真正掌权的又是谁？我们已经讨论过比特币的基础是人们对它达成的共识以及它的规则手册是如何编写而成的，分析过分叉的可能性以及因为对规则存在异议而可能引发的斗争，那么，谁有权决定斗争的胜利者呢？现在我们来谈谈这个问题。

换言之，如果比特币社区存在关于规则设定的讨论和谈判，而谈判失败了，我们想知道谁将对最终结果有决定权。通常来说，在一场谈判中，对谈判协议拥有最佳选择的一方具有优势。因此，搞清楚谁更有可能获胜，将帮助我们了解谁会在关于比特币未来的讨论和谈判中占据上风。

我们代表许多不同的利益相关者做出如下声明：

1.比特币核心钱包首席开发人员拥有权力——他们编写规则手册，几乎人人都要使用他们的代码。

2.矿工拥有权力——他们编写历史记录，决定哪些交易是有效的。如果矿工选择某一套特定的规则，理论上来说，其他人也必须要遵守它。拥有更强采矿能力的分叉将创建一个更强大、更安全的区块链，因此，更有能力把规则朝某一方向推进。矿工到底拥有有多大的权力取决于分叉是硬分叉还是软分叉，但不管是哪种分叉，他们都是拥有一定权力的。

3.投资人拥有权力——他们购买并持有比特币，决定了比特币是否具有价值。可以说，开发人员决定了对规则的共识，矿工决定了对历史记录的共识，那么，投资人决定了对比特币价值的共识。在硬分叉的情况下，如果大多数投资人决定把他们的钱投入货币A或货币B中，那么

该特定分支就被认为是合法的。

4.商家及其客户拥有权力——他们构成对比特币的主要需求。我们在第4章中讨论过，虽然投资人能够一定程度上支持货币价格，但推高货币价格的主要需求来源于将比特币作为一种支付技术促成交易的需求。因此，投资人只是对未来比特币的需求做出推测。

5.支付服务商拥有权力——它们处理交易。许多商家并不在意它们使用的是哪种货币，它们只想与一家支付服务商合作，支付服务商允许顾客用加密数字货币进行支付，承担全部风险，并在每日结束时跟自己结账。因此，很有可能是支付服务商构成了主要需求，商家、顾客和投资人只是跟随者。

你可能已经猜到了，这些观点都有其合理性，所有这些群体都有一定的权力。要想成功，一种电子货币需要以下不同形式的共识——由开发人员编写的稳定的规则手册、采矿能力、投资、商家和顾客的参与以及支持他们的支付服务商。所以，所有这些参与方都对影响比特币未来发展的斗争结果有一定的话语权，但没有哪一方是拥有绝对控制权的。这是一个庞大、曲折且混乱的建立共识的过程。

另一个与比特币管理相关的组织叫比特币基金会（the Bitcoin Foundation），它成立于2012年，成立之初是一家非营利组织。现在它主要扮演两个角色：其一，它从资产中拿出一部分资助比特币核心钱包开发人员，以便他们可以全力以赴开发软件；其二，它与政府，特别是与美国政府沟通，作为比特币的发声机构。

现在，比特币社区的一些成员认为，比特币的运行应该游离并独立于传统的国家政府。他们认为比特币应该跨国运行，它不需要向政府解释或证明自己，也不需要与他们谈判。其他人则不这么认为。他们认为被监管无法规避，甚至是有益的。他们希望政府了解比特币社区的利益所在，听到比特币社区的声音。比特币基金会的诞生部分是为了满足这

个需求，可以说，比特币被人们理解和接受，很大程度上要归功于比特币基金会一直以来与政府之间的沟通工作。



开放协议（open protocol）的治理

我们已经对比特币系统进了一些描述，在这个系统中，利益并不完全一致的众多利益相关者在开放协议和系统中相互协作，达成技术上的和社会性的共识。这可能让你想起互联网本身。比特币核心钱包和互联网的发展过程确有共同之处。例如，BIP就类似于“评议请求”（Request for Comments，简称RFC），RFC是一种用于设置互联网标准的文件。

比特币基金会一直备受争议。基金会的一些董事会成员卷入了犯罪或金钱丑闻，人们对他们在多大程度上能代表比特币社区存在疑问。基金会面临着要迅速调整此类将带来负面影响的董事会成员，但这会带来挑战。人们指责它缺乏透明度，而且正在迅速走向破产。截至2015年，比特币基金会能够在比特币的未来发展中发挥多大的作用尚不明确。

另一个非营利性组织“货币中心”（Coin Center）成立于2014年9月，总部位于华盛顿特区，承担了比特币基金会的部分职能，充当宣传和与政府沟通的角色。货币中心的运作类似一个智囊团，截至2015年年初，它受到的争议较小。比特币基金会和货币中心对比特币的控制权都比不上其他的任何一方利益相关者。同开源代码的生态系统中的所有事物一样，这种代表性实体机构是否能成功、其合法性能否获得公众认可，取决于随着时间的推移，它们能够在比特币社区获得多少支持和资金。

总之，还没有一个实体机构或群体对比特币的演化拥有绝对的控制

权。从另一种意义上来说，每个人都能够决定比特币未来的演化，因为管理比特币的正是人们对比特币系统如何运作所达成的共识——对规则、历史记录和价值这三个相互关联的方面所达成的共识。任何一种规则集合、群体或管理架构，只要能够维持在这三方面的持久共识，就能够在真正意义上决定比特币的未来。

7.4 比特币的起源

现在我们来谈一谈比特币的起源。它是如何开始的？它的前身是什么？我们对其神秘的创始人了解多少？

密码朋克和数字货币

比特币其中一个值得一提的前身是密码朋克（cypherpunk），一项汇聚了两种观点的运动。首先是自由主义，特别是认为如果没有或者极少政府干预会让社会更好的观点。其次，该运动与自由主义者（甚至是无政府主义者）的概念联系在一起，加上强加密的想法，特别是于20世纪70年代后期出现的公钥密码学。参与密码朋克运动的人们相信，拥有了强大的网络隐私和强加密，他们可以重塑人们相互交流的方式。密码朋克认为，在这个世界上，人们应该更加有效地保护自己和自身权益，少受政府行为影响（或干预）。

密码朋克遇到的一个难题是，在他们所构想的未来世界中，人们通过强大的技术和加密手段进行网上沟通时，如何解决金钱相关的问题。许多研究都是为了探讨这个问题，特别是大卫·乔姆（David Chaum）和其他人所做的关于数字货币（digital cash）的早期研究工作，他们试图创建一种具有现金的功能、能够匿名使用和极易交易的新型数字货币。这些技术性的想法是如何发展、数字货币又为何没能流行开来，这背后是一个有趣的故事（参见前言部分）。该领域的所有前期工作都与密码朋克的信仰密不可分，特别是他们对拥有去中心化的、线上和相对私密的强势货币的愿望，都为比特币的诞生播下了种子。它也是很多比特币追随者所遵循的理念基础。

中本聪

2008年，中本聪发表题为“比特币：一种点对点的电子现金系统”的白皮书，宣告了比特币的诞生。白皮书当时可以在网络上自由下载，是第一篇描述比特币的运作模式和设计理念的文章。现在，它依然可以帮助人们迅速了解比特币的技术设计和理论基础。中本聪随后发布了实现白皮书中规范的开源软件，这正是一切的开端。时至今日，中本聪的身份依然是关于比特币的最大谜团。

重要的是，我们不知道中本聪的身份并不是什么要紧事，因为比特币的显著特点就是它的去中心化，而且不受任何单一实体控制。中本聪并不是掌权人，事实上，自从2010年年中将比特币的控制权转让给其他开发者之后，他便不再积极从事这个项目了。从某种程度上来说，中本聪到底在想什么已经不重要了。如果中本聪再度活跃起来，他在比特币社区的声望可能会影响社区的决策，这是他唯一的影响力。

增长

自2009年1月正式上线以来，比特币已经取得了大幅度增长。我们从一段时期的交易走势（见图7.3）和一段时期的交易数量（见图7.4）中都可以很清楚地看到这一点，尽管有过一段时期的滑落，但2013年下半年又开始企稳，并于2015年达到峰值。虽然有时候，增长是渐进的，但也有激增的情况，通常是在新闻事件发生之后。总的来说，长期看增速是加快的。



谁是中本聪？

几乎可以肯定“中本聪”是一个笔名。中本聪自称是一名生活在日本的37岁中年男性。但是，目前没有证据表明中本聪说日语或懂日语，但是他的英文书写相当流利，尽管美式拼写和英式拼写混在一起。有不少人研究中本聪的文章、代码、发表时间、机器标识符等蛛丝马迹，试图以此回答中本聪的母语是什么，他来自哪里。有些人甚至尝试通过文体计算（对作家风格进行文字算法分析）来找出中本聪的身份。虽然有些人自称是中本聪，甚至一家新闻媒体也曾这样宣称过，目前，中本聪的真实身份仍是未知数。请参考前言部分关于中本聪的更多讨论。



图7.3 比特币的市场价格（7天的平均值）

注：注意计算尺。

资料来源：bitcoincharts.com

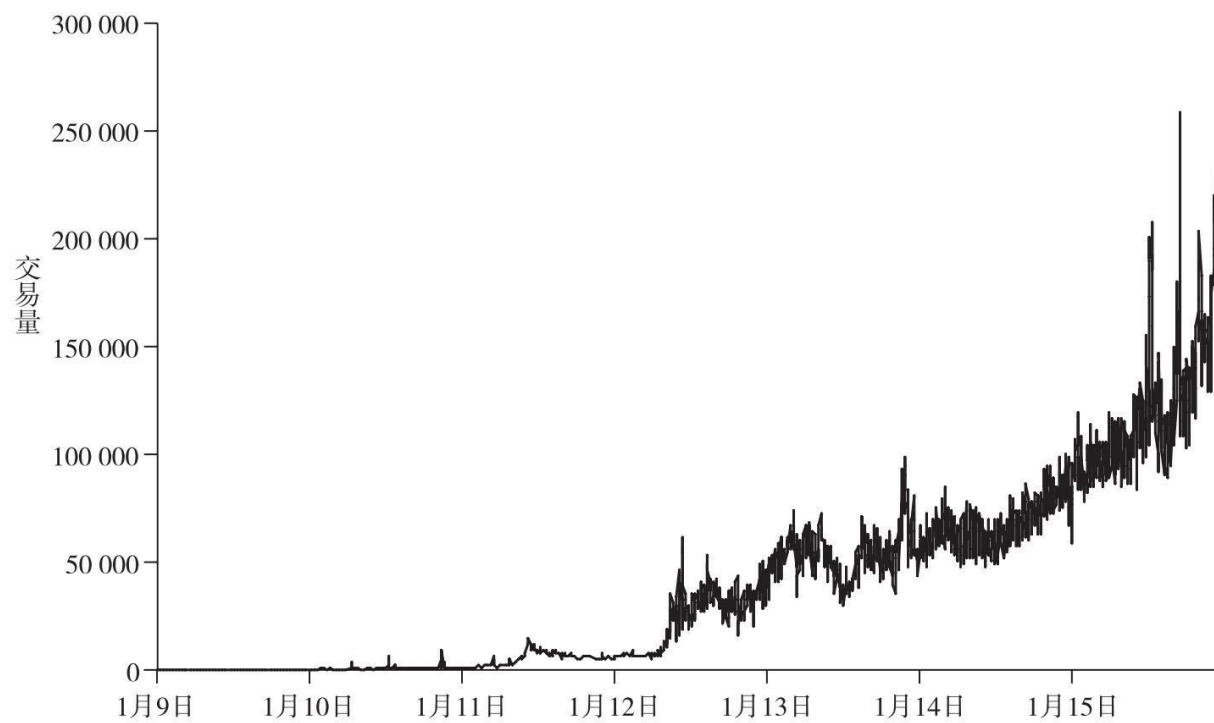


图7.4 日均交易量（7天平均值）

资料来源: bitcoincharts.com

7.5 政府对比特币的关注

本章接下来的内容我们将谈谈政府，政府与比特币的关系以及为监管比特币所做的努力。随着比特币成为一个足够庞大的现象，政府才开始注意到比特币，并开始担忧它可能造成的影响以及自己应该如何应对。本节和下节内容，我们将讨论为什么比特币会让各国政府产生担忧。在7.7节，我们将参照其他被监管的业务，讨论比特币可能会被监管的原因。7.8节将对一个结合了常规消费者权益保护和比特币特性的监管提案进行案例分析。

资本管制

政府之所以注意到比特币这样的数字货币的原因之一在于，不可追踪的数字货币不受资本管制。资本管制是指一个国家颁布法律或法规，以控制流入或流出该国的资本（货币或其他资产）。通过对银行和投资行为等设置限制性条件，国家可以监管资金流动。

在某些情况下，比特币可以轻而易举地绕过资本管制。人们可以在某国境内购买比特币，把这些比特币以电子方式转移到境外，然后将其兑现成资金或财产。这样，他们可以把资金或财产从境内转移到境外，或从境外转移到境内，而不受政府的管制。因为财产可以通过这样的电子方式轻而易举地进行跨境转移，而且无法真正被管控。政府如果想对比特币进行监管，就必须把比特币与当地法定货币银行系统隔离开来。这样，把大量当地货币兑换成比特币或反过来的做法就行不通了。一些试图进行资本管制的国家确实是这么做的，有些国家采取强硬措施，不允许企业用比特币换取当地货币，试图把比特币与法定货币银行系统隔离开来。

犯罪

不可追踪的数字货币让政府担忧的另一个原因是，它使某些犯罪更加容易，特别是涉及支付赎金的犯罪，例如绑架和勒索。如果可以从远程匿名支付，这些犯罪会更加容易。

例如，打击绑架的执法人员往往依靠受害者或其家人向绑匪转账的记录提供追查线索。远程匿名转账会加大执法人员追查转账流向的难度。还有一个例子，CryptoLocker软件可以对受害人的资料恶意加密，并要求必须用比特币支付赎金才可以解密。这样，犯罪行为 and 支付行为都可以远程进行。同样，当人们可以很轻松地转账，参与的交易并不需要与某个特定的个人或组织绑定时，逃税对他们来说也更加方便了。最后，如果远程转移资金可以不通过监管机构，出售非法商品就会更加容易。

“丝绸之路”

丝绸之路公司（Silk Road）^[1]就是一个很好的例子，它自称“匿名市场”（anonymous marketplace），被称为“销售非法药品的易贝网”。图7.5是“丝绸之路”的网站截图。毒品是它的主要销售商品，在网页右侧还可以看到为数不多的其他类别的在售商品。

卖家可以在“丝绸之路”宣传自己的商品，买家则可以购买它们。商品通常通过邮寄或货运的方式发到买家手中，支付方式为比特币。网站以Tor隐匿服务的方式运作，我们在第6章已经讨论过这个概念。从截图中我们可以看到，网站地址为<http://silkroadvb5piz3r.onion>。这样，执法人员也无法追查到服务器的位置。

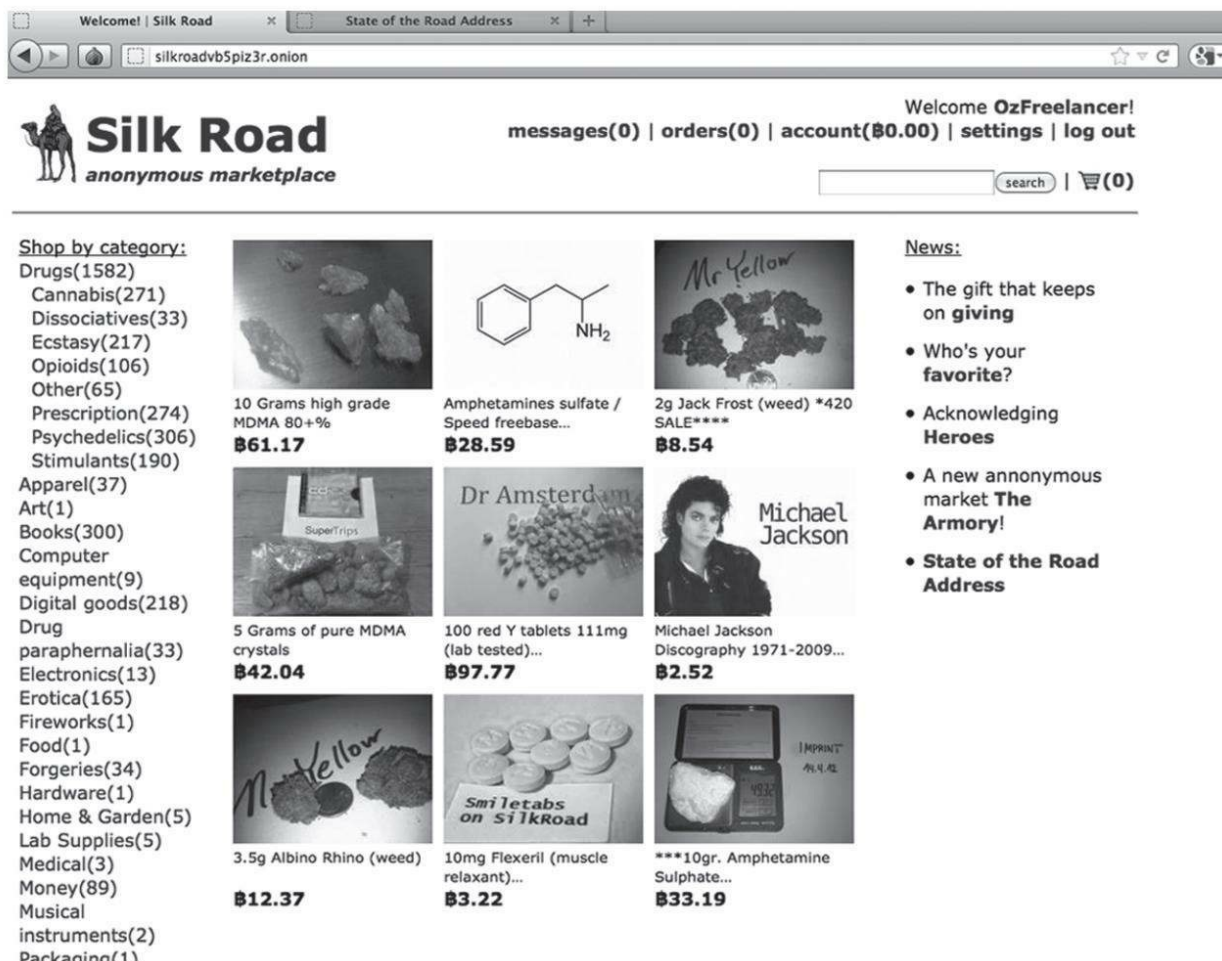


图7.5 丝绸之路公司网站的截图（2012年4月）

由于交易是通过比特币支付的，执法人员也很难追查资金流向，查出哪些人参与其中。商品发货时，“丝绸之路”网站暂为代管比特币。这个极具创新性的代管机制有助于防范买家和卖家被对方欺骗。买方确认收货之后，网站才会把比特币转给卖方。它还有类似于易贝的信誉评价系统（reputation system），买家和卖家在交易完成之后获得信誉评级。因为这个信誉评价系统，“丝绸之路”鼓励买卖双方以符合市场规则的方式进行交易。因此，作为一个非法购物网站，“丝绸之路”是很有创新性的，它找到了一条以遵循市场规则进行远程非法交易的道路，而之前的非法市场很难做到这一点。

“丝绸之路”由一个自称“恐怖海盗罗伯茨”（Dread Pirate Roberts）的

人运作，这显然是一个化名，极有可能来源于小说或电影《公主新娘》中主人公的名字。网站自2011年2月开始运行，2013年10月，它的运营者、后被认定就是“恐怖海盗罗伯茨”的罗斯·乌布利希（Ross Ulbricht）被逮捕之后，网站关闭。乌布利希曾试图通过使用多个化名账户、Tor及匿名重发（anonymous remailers）等方式掩盖自己的踪迹。尽管如此，美国政府还是将种种蛛丝马迹联系在一起，证据表明他与“丝绸之路”的活动、网站服务器以及作为网站运营者所控制的比特币之间存在密切联系。他被判犯下与运营网站相关的多项罪行。他的罪行还包括买凶杀人，幸运的是，他在这方面的能力实在太欠缺，并没有人被杀害。

在打击“丝绸之路”的过程中，联邦调查局收缴了约174 000比特币，当时市值超过3 000万美元。根据美国法律，政府有权没收任何犯罪所得收益。后来，政府拍卖了部分收缴的比特币。

“丝绸之路”的教训

从执法人员和“丝绸之路”的较量中，我们可以吸取一些教训。第一，把现实世界和虚拟世界完全分离开是很困难的。乌布利希认为自己可以既拥有现实生活，又可以用一个秘密身份来经营庞大的业务和技术设施。事实上，把这两个世界分开，让二者不存在任何一丝联系，是很难做到的。活跃地参与到一些需要与他人协调的活动中，同时想长期保持匿名，这会非常困难。一旦两种身份之间出现了一些联系，比如，如果你穿帮了，可能会用另外一个身份来为此打掩护，这种联系永远不会消失。这样，随着时间推移，一个人所使用的不同身份就会渐渐有了关联性。这正是发生在乌布利希身上的事情——他在早期用同一台计算机访问自己的个人账户和“恐怖海盗罗伯茨”账户。这些错误最终为调查人员提供了线索，发现他的现实身份。

另一个教训是执法人员可以对资金进行追踪。在乌布利希被捕之

前，联邦调查局就已经知道“丝绸之路”运营者管理着的比特币地址，他们一直监控着这些地址。因此，尽管乌布利希的区块链拥有大量财富，他无法从这些财富中收益，因为只要他试图转移资产，就会留下可追踪的痕迹，很可能会导致他迅速被捕。因此，尽管乌布利希拥有174 000比特币，在现实生活中，他并没有过上奢侈的生活。他居住在旧金山一个一居室的公寓里，显然，他无法将自己积累的财富兑现。

简而言之，如果你有意经营一家秘密的犯罪公司——当然，我们并不推荐这条“事业”道路——做起来可能要比你想象中难得多。比特币和Tor这样的技术并不是刀枪不入的，执法部门仍然拥有很多重要的手段帮助侦破案件。尽管执法部门对比特币的崛起有过一定恐慌，但它们依然可以对资金进行追踪，而且也具备侦破犯罪案件的强大能力，让那些从事需要与他人协调的犯罪行为的人日子不那么好过。

同时，“丝绸之路”是关闭了，但执法部门并没有完全关闭通过比特币交易的经营非法药物的黑市。事实上，“丝绸之路”关闭之后，这类黑市如雨后春笋般涌现，其中一些较为突出的黑市包括绵羊集市（Sheep Marketplace）、“丝绸之路2.0”（Silk Road 2）、黑市重装上阵（Black Market Reloaded）、进化（Evolution）和阿格拉（Agora）。由于执法人员的行动或者内部人员的偷窃，其中大多数现在已经不复存在。虽然如此，研究发现，执法部门对这种黑市的打击并未使其放缓增长，其销售额反而上涨。网站经营者可能私吞买家被代管的资金，然后消失。为了规避这种安全风险，新出现的集市多采取多重签名代管（我们在第3章已讨论过），不再采用“丝绸之路”由经营者保管资金的方式。

[1] 丝绸之路公司是一个利用Tor的隐秘服务来运作的黑市购物网站。2013年，美国FBI捣毁了丝绸之路公司，并且逮捕了该网站创始人。——编辑注

7.6 反洗钱

这本节中，我们将讨论洗钱和反洗钱相关法律、政府，尤其是美国政府所制定的反洗钱（Anti-Money Laundering,简称AML）法律对比特币相关业务造成的影响。

反洗钱政策的目的在于防止资金的大量秘密外流或流入，防范资金在非法与合法企业或机构之间秘密流动。在7.5节我们讨论过，资本管制是为了防止资金的跨境流动。在某些情况下，政府并不介意资金跨境流动，但它们想知道资金的来源和去向。反洗钱政策的目的是给某些特定类型的犯罪行为增加难度，特别是有组织犯罪。有组织犯罪的罪犯经常会收到大笔资金，需要转移这些资金，但又不想对任何人解释这笔资金的来源，以及为什么想把这笔资金转移到境外。或者，罪犯通过非法活动赚到了一大笔钱，想通过合法企业使其合法化，这样，犯罪头目就可以购买各种奢侈品。反洗钱的目的就是让资金转移更加困难，而且，有人试图这么做时，会更容易被发现。

了解你的客户

“了解你的客户”（Know Your Customer，简称KYC）原则，是打击洗钱活动的根本对策之一。KYC原则的细节有些复杂，而且根据立场不同而有所变化，但其核心思想是，“了解你的客户”原则要求，对于一些有资金处理业务的特定类型的企业，需要做到以下三件事：

1. 识别并验证客户 ——获得客户的身份证明，确定客户的真实身份与他们声称的身份一致，并确保他们声称的身份与现实世界的真实身份对应。一个人推开门直接走进屋，说自己是住在美国某市某街道多少

号的张三、李四，企业不能凭此口述确认他的身份，他必须提供可靠的身份证明文件。

2. 评估客户风险 ——确定客户从事地下行为的风险。通过评估客户行为以确定风险——他们与公司的合作关系是否长久、他们在社区的知名度以及其他多个因素等。通常而言，KYC原则要求公司对看起来风险更大的客户实施监控。

3. 监控异常举动 ——监控看似洗钱或犯罪的行为。如果一个客户看上去不甚可靠，或者无法对其身份进行充分验证，或者其行为没有符合法律的要求，那么KYC原则往往要求公司终止与这种客户的业务往来。

强制上报

美国的强制上报（mandatory reporting）对比特币的业务影响重大。众多行业内的公司被要求必须将超过10 000美元的资金交易进行上报。它们需要提交一份《资金交易报告》，说明交易内容和交易对手的身份，这份报告还要求对交易对手进行身份验证。报告提交后，所有信息纳入政府数据库，以便将来分析是否存在洗钱行为的嫌疑。

美国政府还要求各公司关注那些可能通过人为操控以规避上报交易的客户，比如，由于法规只要求对金额超过10 000美元的交易进行汇报，一些人可能开展数笔金额为9 999美元的交易。如果发现客户操控交易，公司必须编写《可疑行为报告》，并汇报给政府。同样，这些信息也会被录入政府数据库，用于可能对客户开展的调查。

各个国家的要求各不相同。在此，我们并不是想提供什么法律建议。讨论这个话题只是为了说明反洗钱法规提出的一些要求。不管是美国政府还是其他政府，都非常重视反洗钱法规，一旦有人违反，可能会

被判以重刑。有一些法律，违反之后，政府可能会投诉你，然后你再设法去解决它，反洗钱法并不是这样的。

政府已经关闭了许多比特币企业，一些是暂时的，一些是永久的。还逮捕了一些从业人员，也有一些人因为违反反洗钱法而锒铛入狱。不管是使用比特币还是法定货币，国家都会严厉打击洗钱行为。自从注意到比特币市场已经足够大，可能会带来洗钱风险，政府部门就强化了对比特币相关企业可能洗钱的监控。如果你有兴趣创建一家需要处理大额资金的企业，那就需要跟理解这些法规的律师好好谈谈。

7.7 监管

现在让我们来直接谈谈监管问题。监管通常背负恶名，亲比特币派尤其不喜欢这个词。这些人认为，监管是一种官僚主义，它们根本就不了解我的业务，不懂我做的事情，只会横插一脚，把事情搞砸。监管是一种负担，它不仅愚蠢，而且毫无意义。这种观点很普遍，而且容易得到认同，它也许不无道理，但此处我们不再重复了。

相反，在本节中，我们将探讨为什么监管有时是可取的，因为很多人并不理解这种观点。澄清一点，我们虽然在本节要花大量篇幅来解释为什么监管有时是一件好事，这并不代表我们支持对比特币进行全面监管。但是我们想让认为监管生而可恶的社区听到一点不同的声音。

赞成监管的基本原因是：当市场失灵并带来大家一致认可的恶果时，监管可以介入，并解决这种失灵。由于市场并不总是给出最优的结果，所以我们说监管有时是有益的。

我们可以用经济学术语更为准确地表达这一观点。我们担心市场会失灵，“失灵”的意思，并不是说坏事发生，或者有人觉得他们被敲诈或被不公平对待。我们指的是，对市场参与者进行不同的商品分配，这会让每个人更好，或者至少不会更差。这种不同的分配被称为帕累托改进（Pareto improvement）。

柠檬市场

柠檬市场（lemons market, 也称为次品市场）是可能导致市场失灵的一个经典案例。柠檬市场的名称起源于汽车销售行业，但这个概念并不

局限于这个行业。假设所有汽车要么优质要么劣质，没有中间地带。制造一辆优质汽车的成本比一辆劣质汽车的成本高不了多少，但对于购买汽车的人来说好处则多很多。

如果市场运行良好（即经济学家所说的“有效运行”），汽车销售商会向顾客提供更多优质汽车。这是因为，虽然优质汽车价格较高，但大多数消费者更喜欢优质汽车，愿意花更多的钱购买。所以，在假设条件下，市场会提供这样令人愉悦的结果。

但是假设顾客分辨不出哪些汽车是优质的，哪些是劣质的。一辆劣质汽车（一个“柠檬”，俗称次品）从外观上看上去似乎很不错，但顾客不知道它会不会明天就熄火，还是可以开很久。销售商很可能知道它是一个次品，但是顾客是分辨不出来的。

接下来，我们考虑这种柠檬市场是如何驱动人们的消费行为的。作为一名消费者，由于在购买汽车前根本看不出区别，即便销售商告诉顾客这辆车非常好，顾客只需要多掏100美元就可以买下，顾客未必会相信他，也就不愿意掏多余的钱买一辆优质汽车。

由此带来的结果是，生产商并不会因为多卖出一辆优质汽车而多赚一笔钱。事实上，每卖一辆优质汽车，它们反倒赔钱，因为优质汽车的生产成本更高，它们并没有赚到差价。最终，生产商只生产劣质汽车，而顾客对自己所购买到的商品非常不满，市场就卡在这个平衡上。

与正常运行的市场相比，这个结果对每个人来说都更糟糕。它对消费者来说更糟，因为他们不得不凑合使用劣质汽车。在一个运行更加有效的市场中，他们可能只需要多花一点钱，就可以购买到质量好得多的汽车。对于生产商来说也很糟，因为市场中出售的汽车都是次品，消费者可能就不会买那么多汽车，因此，销售汽车获得的利润要比在一个健康市场上的利润少得多。

这个现象就是市场失灵。柠檬市场并不专指汽车行业。任何待售的存在信息不对称（asymmetric information，即买方或卖方中的一方比另一方对商品品质的了解要多）的商品或小部件都会遭遇市场失灵。经济学文献可以提供汽车行业以外的更多案例。

修复柠檬市场

通过一些市场手段，可以修复柠檬市场。一种手段是通过卖方的信誉。如果卖方总是实话实说，告诉买方哪些是优质品哪些是劣质品，久而久之，这个卖方就会被大家认为是诚实的。一旦有了这种信誉，它们就能够以更高的价格出售优质汽车，因为消费者会相信它们说的话，市场也就可以更有效地运行。这一手段有时奏效，有时无效，取决于对市场所做的假设是否准确。当然，它即便有效，也比不上消费者能够分辨商品质量好坏的市场。而且，生产者需要一段时间才能建立自己的信誉。这也就要求它们必须要在一段时间内以低价销售优质的商品，直到消费者意识到它们的诚实可靠。这加大了诚信卖家进入市场的难度。

还有另外一个潜在问题，即便是一个一直有诚信的卖家，当它决定退出市场（比如因为销售额下降）时，就不再有动力继续对买方说实话。它可能会趁机大肆欺骗买方，然后关门大吉。因此，在卖家一开始进入市场或决定退出市场时，通过卖家信誉来修复柠檬市场的方式并不一定奏效。

对于消费者不会从同一个买家重复购买商品的行业，或者商品是新兴事物，卖方还没有足够的时间建立起信誉的行业，通过信誉修复柠檬市场的手段也很可能不会奏效。像比特币这样的高科技市场就面临这样的问题。

另一种修复柠檬市场的手段是担保。卖家向买家提供担保，也就

是，如果商品最终被证明是劣质的，卖家会换货或退款。这种方法是比较有效的，但也存在一个问题：担保也是另一种可能存在质量高低的商品！如果是一个劣质担保，当购买的商品出现问题后，卖家可能根本就不兑现之前的承诺，或者在买家要求兑现担保承诺的过程中故意设置各种难题。

通过监管手段修复

如果确实存在一个柠檬市场，而且上述所有的市场手段均未奏效，那么监管可能会帮上忙。具体来说，监管可以通过以下三种方法修复柠檬市场。

第一种方法是，监管可以要求信息公开。比如，可以要求所有的汽车都贴上标签，标明它是优质汽车还是劣质汽车，并对造假的企业施以处罚。这可以让消费者了解他们之前并不了解的信息。第二种监管方法是出具质量标准，只有通过质量标准检测的汽车才可以出售，否则不得出售。有了这样一个标准，只有优质汽车才能够通过质量检测。如果监管奏效，可能会导致市场上只有单一质量的汽车，但至少都是优质汽车。第三种方法是，监管可以要求所有的销售方出具担保，并强制执行这些担保，这样，销售方就必须对其做出的承诺负责。

所有这些监管手段都可能失效，它们可能达不到预想效果，可能会写得不好、误用，或者对卖家造成负担。但是这种监管为柠檬市场导致的市场失灵问题提供了一个可能的解决方案。例如，一些支持对比特币交易市场进行监管的人，有时就认为它是个柠檬市场。

串谋和反垄断法

市场不以最优方式运作的另一个例子就是价格垄断。价格垄断是指不同卖家相互串通，一致上调或下调价格的做法。另一个与之相关的情况是，本应该是竞争关系的公司决定不再相互竞争。例如，某市有两家面包店，它们商量好，一家只卖松饼而另一家只卖面包圈，这样，比它们两家同时既卖松饼又卖面包圈的竞争要小得多。竞争减少，商品价格自然上涨，商家对市场的运行造成阻碍。

总之，一个正常运转的市场主要通过竞争来保护消费者权益。卖家必须以最优惠的价格向顾客提供最好的产品来进行竞争，否则，它们就没有业务。价格垄断或串谋行为规避了竞争。如果人们采取措施规避竞争，这是另一种形式的市场失灵。

在大多数司法管辖区，商量好涨价或者不竞争的行为是违法的。这是反垄断法或竞争法的一部分内容。这一法律的目的是限制蓄意阻碍或损害竞争的行为。一般来说，它更侧重于限制诸如通过并购减少竞争的行为，而不是为消费者提供物美价廉的商品。反垄断法很复杂，我们只做了一些简单介绍，但它为市场失灵后，法律如何介入并纠正市场失灵提供了一个案例。

7.8 纽约州比特币牌照

截至目前，我们已经对监管内容做出了概述：监管的不同形式，为什么在某些情况下监管是有利于经济运行的。接下来，我们来看看纽约州比特币牌照（Bitlicense），这是某个州对比特币监管所做出的一项具体努力。此处描述的细节对于我们的讨论影响不大，因为我们的目标并不是让你了解一个法律条款。相反，我们希望帮助你了解监管部门都在做哪些事情以及它们是如何考虑这些问题的。

《纽约州比特币牌照提案》最初于2014年7月提交，后续根据比特币社区、行业、公众以及其他利益相关者的反馈进行了修订，最后由州立监管金融行业的纽约州金融服务管理局（New York Department of Financial Services，简称NYDFS）于2015年8月颁布施行。当然，纽约州是世界最大的金融中心，州金融服务管理局也习惯与大型金融机构打交道。

涉及范围

《纽约州比特币牌照提案》是一套关于虚拟货币（virtual currency）的规范、法规和规章制度。它要求，如果你想要从事以下任何事情，那么必须从纽约州金融服务管理局获得所谓的比特币牌照：

虚拟货币业务行为是指涉及纽约州或纽约州居民的以下类型的行为：

1. 接收虚拟货币用于传输或传输虚拟货币，交易用途为非金融性且不涉及超过虚拟货币面额的转移除外。

2. 存储、持有或为他人代管虚拟货币。
3. 为客户提供购买或销售虚拟货币的服务。
4. 为客户提供兑换服务。
5. 控制、管理或发行虚拟货币。

内部员工或其本身对软件的开发与传播，并不属于虚拟货币业务行为。

（摘自纽约金融服务管理局的《纽约州比特币牌照提案》的原文。）

以上条款是指“涉及纽约州或纽约州居民的行为”，反映了纽约州金融服务管理局的监管权力。然而，这种法规不仅对纽约州，对其他州也造成影响，原因有二：第一，在面临要么遵守州的法律，要么放弃在该州的业务时，像对纽约或者加利福尼亚这样人口众多的州，大多数公司都会选择遵守州法。第二，在对一些经济领域的监管上，一些州通常被视为领导者——纽约州在金融领域、加利福尼亚在科技领域。这也就意味着，美国其他州会沿着领导者设定的方向走下去。

请注意第一条提到，“交易用途为非金融性的除外”，这是在第二版修订中增加的，这一点加得很好，它剔除了那些仅把比特币当作平台的应用程序，我们将在第9章探讨。第二条涵盖了钱包服务。至于第三条，你可以为自己购买和出售比特币，但是把它作为业务向顾客提供服务则需要获取比特币牌照。第四条足够清晰明白。最后一条可能更适用于另类币，与比特币相比，许多另类币的中心化更强。我们将在第10章中讨论另类币。

在条款的最后，把软件开发作为例外特别声明，也是非常重要的。在最初版本中并不包括这句申明，引发了比特币社区的强烈抗议。纽约州金融服务管理局局长本杰明·劳斯基（Benjamin Lawsky）随后做出解

释，申明本条款的目的并不是为了监管开发人员、矿工或使用比特币的个人。最终版本包含了上述两个明确的例外情况。

要求

相关实体都必须申请一个牌照。你可以在提案中找到关于如何申请牌照的详细规定（参见本章最后的“延伸阅读”），但是简而言之，你需要提供一些充分的材料，证明你对企业的所有权、经济状况、保险和商业计划，以便让纽约州金融服务管理局了解你是谁、你是否有足够诚信、你的经济来源以及你打算用此做什么。此外，你还需要支付一笔申请费。

获得牌照后，你还需要向纽约州金融服务管理局提供所有权、经济状况、保险等信息。你还必须定期提供财务报表，以便让它们了解你的经营状况。你还需要维护一笔财务储备金，纽约州金融服务管理局会根据你的业务具体情况，确定具体金额。

提案包含如何监管客户资产等内容，也有非常详细的条款。提案也包括反洗钱条款，其内容可能与现有法律一致，也可能比现有法律规定的内容更多。提案包括关于安全计划和渗透测试等方面的条款；还有一些关于灾难恢复预案的条款，规定了必须制订灾难恢复计划以应对一切可能发生的糟糕情况；包括了历史记录保存的相关条款，申请者必须要保存记录，并允许纽约州金融服务管理局在某些情况下对其进行访问；申请者还必须制定合规的章程，在组织内部任命专门的合规员，并赋予必要的权力，确保业务的合规性。此外，申请者还必须向客户披露风险，让他们了解与申请者进行业务往来可能存在的风险。

正如你所看到的，提案要求的名目繁多，与成立共同基金或股票上市所要满足的要求极为类似。因此，比特币牌照是比特币历史上关键的

一步。可能还有其他部门也会开始介入比特币的监管，然后比特币业务就会越来越接近传统的受监管的金融业务。

这可能会跟密码朋克和密码自由主义者对比特币的期望背道而驰。但这可能具有一定的必然性，因为随着比特币价值的增加，比特币业务将会越来越大，政府会对它们产生兴趣，监管也就随之而来。比特币业务会对现实世界的人们及实体经济产生影响。如果比特币发展到了这种程度，也就意味着它已经发展到了需要被监管的程度。它表明比特币最初簇拥者的理念开始淡出，但另一方面，它也表明比特币生态系统在不断壮大，并且正在与受到更严格监管的实体经济不断融合。不管你对此持何种态度，对比特币的监管正在发生，如果你有兴趣创立一家比特币公司，你需要关注这一趋势。

这种监管比特币的努力会成功吗？可以有不同的方式来看待它，但是有一种方式，可以从提升比特币业务质量的角度，来评估像比特币牌照这种监管措施的有效性：如果企业在向非纽约州的客户推广业务时申明，它们拥有比特币牌照，因此它们是可以信赖的。假如企业的申明会让客户信服并由此开展业务往来，那么监管措施正如它的支持者设想的那样，发挥了作用。这个场景是否会发生，以及监管措施究竟会产生什么样的影响，让我们拭目以待。

延伸阅读

关于“丝绸之路”及其后继者的运作模式的两篇论文：

Christin, Nicolas. “Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In Proceedings of the 22nd International Conference on the World Wide Web , New York: ACM, 2013.

Soska, Kyle, and Nicolas Christin, “Measuring the Longitudinal

Evolution of the Online Anonymous Marketplace Ecosystem.”In Proceedings of the 24th USENIX Security Symposium, Berkeley, CA: USENIX, 2015.

以下是比特币监管问题指南：

Brito, Jerry, and Andrea Castillo. Bitcoin: A Primer for Policymakers . Fairfax, VA: Mercatus Center at George Mason University, 2013.

一本讲述比特币社区及其主要特征的非技术性著作：

Popper, Nathaniel. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money . New York: Harper, 2015.

一篇阐述数字货币的早期作品，探讨了未来世界如何保护数字隐私问题：

Chaum, David. “Security without Identification: Transaction Systems to Make Big Brother Obsolete.” Communications of the ACM , 28 (70) , 1985.

一项对信息安全经济学的调查，其中讨论了市场失灵的一些原因：

Anderson, Ross, and Tyler Moore. “The Economics of Information Security.” Science 314(5799), 2006.

讨论比特币的经济问题和监管方案：

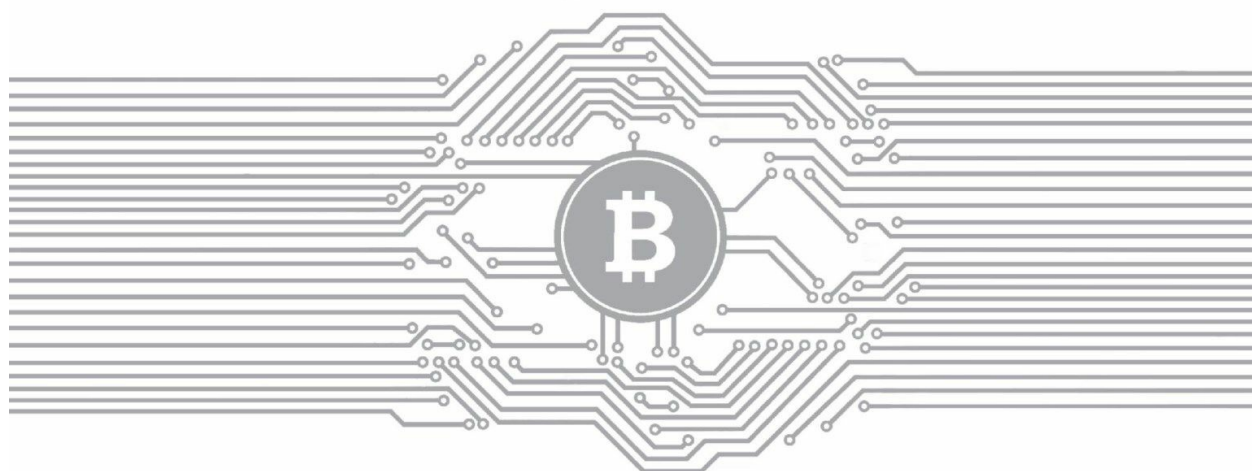
Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. “Bitcoin: Economics, Technology, and Governance.” Journal of Economic Perspectives 29(2), 2015.

《纽约州比特币牌照提案》文本：

New York State Department of Financial Services“Regulations of the Superintendent of Financial Services.Part 200:Virtual Currencies.”2015. 下载地址：<http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.

第8章

其他挖矿算法



由于挖矿算法的复杂性使得任何个人或团体都难以操控共识成形的过程，挖矿算法被认为是比特币系统的核心。因为比特币矿工通过解谜来获得奖励，所以我们可以期望他们会花大量的时间与精力去寻找捷径而更加快速有效地解谜，以增加他们的收益。另一方面，如果有些工作对网络有利但并不能让矿工更快速地解谜，他们可能会忽视那些工作来最小化他们的成本。所以解谜的设计对引导和指引矿工起着至关重要的指导作用。

在本章中，我们会讨论一些其他的挖矿解谜（mining puzzle）设计，假设我们可以改善比特币的解谜甚至重新设计一套新的解谜过程。一个经典的设计挑战是让解谜过程能够限制ASIC挖矿，这样一来可以平衡计算机设备性能上的差距（拥有一般电脑的矿工与拥有优化过的ASIC矿工之间的设备差距）。还有什么其他设计是需要我们考量的？有哪些行为需要我们鼓励，而哪些需要阻止？我们会讨论一些有着不同

特征的案例，从减少能源消耗（这对社会发展有着积极意义），到约束挖矿工具的形成。有一些已经被另类币所采用，另外一些还处于理论研究阶段，可能将来会被用到。

8.1 算法的基本要求

我们首先来看一下一些挖矿算法的主要安全要求。如果算法本身不能满足比特币安全性上的基本要求的话，我们也没有必要引入一些新奇的特点。

已经有许多可能的要求，有些我们在前面的第2章和第5章中已经讨论过。挖矿解谜的结果需要被及时验证，因为每个在网络上的节点都在验证每个解谜的结果，即使是那些没有直接参与挖矿的节点，包括SPV（简单支付验证）的客户端。我们还需要解谜的难度具有可调整的特征，解谜难度可以随着新加入用户而增大的哈希算力得到调整。这样一来，解谜过程就可以具备足够的难度使得对区块链的攻击变得代价高昂，同时又能保证解谜本身可以在一个稳定的频率上实现（比特币系统中大约每10分钟完成一个解谜过程）。

到底什么是比特币的挖矿解谜？

到现在为止我们一直在用“比特币解谜”这个名称，更加精确的说法是，我们称它为一个“不完全哈希函数原像解谜” (partial hash-preimage puzzle)，因为这个运算的目的，是找到一个不完全的特定哈希函数输出值的原像——也就是一个低于某一特定目标区值的结果。除此之外，一些罕见的特征也可以用来作为比特币的挖矿解谜运算，比如找到一个区块，它的哈希函数值至少有k个点位是零，但是通常直接比较既定目标是最简单的方法。

比特币用的基于SHA-256挖矿解谜哈希函数，很显然已经满足了这两个要求。它可以通过任意调节一个参数（目标）来灵活增加难度。检查这个谜底很容易，只需要一个SHA-256计算和一个与目标的比较即

可，不管找到这个谜底的过程有多么困难。

另外一个核心的要求更加微妙：在任意单位时间找到一个谜底的功率，大致上要与所贡献的哈希算力成比例。这就意味着，大矿工虽然拥有非常强大的挖矿机，他也只是有着一定比例的优势来成为下一个找到谜底的矿工。即使是小矿工，也会有一定的机会能够成功并且获取奖励。

为了说明这一点，我们先来设想一个没有满足这个要求的不合格解谜过程。想象一下某一个挖矿解谜要经过精确的 n 个步骤找到一个谜底。例如，不同于我们当前要求的“找到一个SHA-256结果低于某一个固定目标的区块”的做法，如果要求计算 n 个连续的SHA-256函数值，这种做法检查结果会变得没有效率，但是这个问题目前无关紧要，更大的问题在于，因为这个解谜过程需要精确的 n 个步骤来完成，所以网络上解谜更快的矿工将会永远是获得下一个奖励的赢家。很快这个情况就变得路人皆知，最快的矿工会完成所有解谜，而其他矿工完全没有动力继续参与下去。

再次声明，一个好的解谜方案，是给每个矿工一个按比例性的成功概率来赢得下一个谜底，这个概率是与他们所贡献的哈希算力成比例。就好比往一个不同大小色块组成的目标板上随机地掷飞镖，每个不同大小色块就类似于不同矿工所具有的挖矿运算能力。如果你考虑到这一点，这就意味着你猜中谜底的概率并不取决于你已经做了多少工作去解谜（因为大矿工们总是会做更多的工作量）。所以一个好的解谜是“无关过程的”（progress free）[\[1\]](#)。

从数学角度来看，一个好的挖矿解谜一定是一个“无记忆进程的”（memoryless process）——而任何其他的方法都将由于过去的挖掘工作，不可避免地一定程度上奖励挖矿工人。因此，任何可行的解谜从根本上都是一个不断试错的过程（trial-and-error）。这种解谜所需要

的时间，必然服从一个指数分布^[2]，我们曾在第2章讨论过。

可以调整的难度、快速验证和无关过程属性，是比特币挖矿解谜的三大核心特征。基于SHA-256算法的“不完全哈希函数原像解谜”显然满足了这三大要求。有些人可能会说其他一些特征也很重要，我们在后面讨论其他潜在功能的时候会提及。

^[1] 意思是来得早，不如来得巧，但这个巧后面的学问就大了。——译者注

^[2] 旅客进入机场的时间间隔也是一个指数分布，后面进来一个人的时间间隔与前面进来人的时间间隔无关。——译者注

8.2 反ASIC解谜算法

首先我们从讨论设计一个可以反ASIC解谜(ASIC-resistant puzzles)的挑战开始，这个挑战也是最被广泛讨论和追求的可替代目前比特币挖矿解谜的一种。我们在第5章中讨论过，比特币挖矿最初是用普通电脑，然后再升级到GPU和定制化的FPGA设备，到现在基本上由非常强大的优化过的ASIC芯片所垄断。现在的ASIC的挖矿运算能力比一般电脑甚至早期的ASIC都要高太多。一般的电脑即使硬件本身是免费的，也会因为电费价格等因素而变得不可行。

这个转变意味着，在比特币生态系统里的大部分个体（例如使用比特币交易的客户和商家）已经无法参与到挖矿过程中了。有些人认为这是一个危险的势头，一小部分职业矿工控制了整个挖矿的过程。在中本聪最初有关比特币的论文里，用到过“一个CPU一票”的说法，这个说法时不时被有些人用来说明比特币应该是一个被全部用户所拥有的民主系统。

其他人觉得ASIC的崛起是不可避免的，而且这也不会伤害到比特币，这种希望实现反ASIC的愿望也只是有些人希望回到“过去的好时光”。对于反ASIC是否可取，我们保持中立的态度，因为只有这样，我们才可以深入讨论一些技术上的挑战和提议的方案，来实现反ASIC的目标。

反ASIC到底是什么意思

大致上说，我们想抑制为了挖矿而特别定制的设备优势。这也可以理解为，设计一个解谜程序，让现有的普通电脑成为最廉价和最有效

率的解谜运算设备。但这在现实中不可能，毕竟所有的通用电脑的中央处理器里已经针对一些特殊目的进行了优化。并不是所有的电脑都有相同的优化配置，并且它们随着时代而改变。比如，过去的10年中，英特尔（Intel）和AMD在芯片里加入特殊指令（通常叫作“增加硬件支持”）来更加有效地计算高级加密标准（Advanced Encryption Standard，简称AES）的区块密码。所以有些电脑在挖矿这个事情上总是会比其他电脑更加低效。另外，很难想象设计一个挖矿解密程序，而这些程序是依赖普通个人电脑诸如音响或显示器这些特性的，所以去除了那些通用特性的具有特殊目的的设备，很可能会更有效率，并且成本更低。

更加实际地说，我们有一个适中的目标：设计一个解谜程序，尽可能地减少最有效率的定制运算设备与通用电脑之间的效率差距。ASIC还是会不可避免地成为更加有效的挖矿机，但我们至少可以将其运算效能限制在一定范围内，从而让个人用户使用他们已有的通用电脑来挖矿仍具备一定的经济效应。

刚性内存解谜

大多数被设计成反ASIC的解谜程序中，最普遍被应用的叫作刚性内存解谜（memory-hard puzzles）——解谜需要大量的内存来计算，而不是靠大量的CPU时间。一个类似但又不一样的概念是内存限制解谜（memory-bound puzzles），花在读取内存上的时间，占据了这种程序大部分的计算时间。一个解谜可以是刚性内存类而不是内存限制类，或是内存限制类而不是刚性内存类，或是二者兼而有之。一个微妙但重要的区别在于，虽然CPU的速度是计算时间的瓶颈，但平行运算大量解谜的成本，还是被内存的成本所左右，或者反之亦然。通常对于运算类的解谜程序，我们要做到刚性内存和内存限制，就需要保证在运算过程中大量的内存被要求使用，使之成为一个限制性因素。

为什么刚性内存解谜或内存限制解谜可以反ASIC？因为用来计算哈希函数的逻辑运算只占了CPU里的一小部分，意思是在比特币的解谜计算里，ASIC不需要执行一些不必要的功能，而只需要执行计算哈希函数的相关功能，所以占了很大优势。另外一个相关因素是，不同的内存性能上的差异（和单位性能的成本）比不同处理器之间运算速度上的差异要小很多，所以，如果我们设计了一个刚性内存类的解谜，计算时需要相对简单的算力但需要大量的内存，这就意味着，解密成本的上升速率将会像内存成本提升速率那样，在一个相对低一些的水平。[\[1\]](#)

SHA-256已经被认定为不是刚性内存解谜算法。它只需要一个小小的256位模块，可以很容易地被放进CPU的注册机里。但设计一个刚性内存类的工作量证明解谜不是一件太难的事。

Scrypt

现在最受欢迎的刚性内存解谜叫作Scrypt[\[2\]](#)，被第二大加密数字货币莱特币以及其他加密数字货币所用。

Scrypt是一个刚性内存的哈希函数，最早是为了加密密码而不容易被暴力破解（比如，反复试错破解），所以挖矿解谜与比特币用的“不完全哈希函数原像解谜”是一样的，只不过用Scrypt取代了SHA-256。

Scrypt在比特币被发明出来之前就已经存在，而且它是用来加密个人密码，这一点让我们对它的安全性有一定的信心。密码的哈希函数化其实与反ASIC有着相似的目的。出于安全性考虑，我们期望，一个有着定制化设备的攻击者不能够比使用一般电脑或者服务器的用户更快地计算密码的函数值。

Scrypt基本上有两个步骤：第一个步骤是在用随机数据填充随机存

取存储器（Random Access Memory，简称RAM）里面的缓存空间；第二步是从这块内存区域里虚拟随机地读取（或者更新）数据，同时要求整个缓存都存储在RAM里面。

```
1 def sscript(N, seed):
2     V = [0] * N // 初始化N长度的缓存区域

    // 往这个区域里充满虚拟随机数
3     V[0] = seed
4     for i = 1 to N:
5         V[i] = SHA-256(V[i-1])

    // 然后从这个区域里虚拟随意地读取
6     X = SHA-256(V[N-1])
7     for i = 1 to N:
8         j = X % N // 根据X，选择一个随机的索引
9         X = SHA-256(X ^ V[j]) // 根据X的索引来更新这个X

10    return X
```

图8.1 Sscript虚拟代码

图8.1展示了一段Sscript的伪代码(pseudocode)来体现核心的计算原则，但我们也省略了一些细节——在实际中，Sscript使用更大一点的数据块，然后用来充满缓存区的算法略微复杂一点。

为了理解为什么Sscript是刚性内存类的，我们先想象一下如果我们要计算同样的值，但不用缓存区V(参见图8.1)。这当然也是可行的——但在第9行代码里，我们需要重新动态地计算值V[j]，这需要进行j次的SHA-256的迭代运算。因为j的值在每次迭代循环里会从0和N-1中虚拟随机地选择，因此这平均需要N/2次SHA-256计算。这意味着计算整个函数需要 $N \times N/2 = N^2/2$ 个SHA-256计算，但是如果使用一个缓存的话，只需要进行2N次运算。因此，缓存的使用将Sscript的时间复杂度从 $O(N^2)$ 转换成 $O(n)$ 。这样一来，只要简单地选一个足够大的N值使得 $O(N^2)$ 的计算

变得足够慢，以此确保使用内存是更快的选择。

在时间与内存之间的权衡

如果没有一个较大的内存缓存，计算Scrypt会变得很慢，但是用较少的内存来增加相对较少的计算还是可能的。假设我们使用一个大小约 $N/2$ 的缓存（而不是 N 的大小），现在，我们只在 j 是偶数的情况储存 $V[j]$ 的值，丢掉那些 j 是奇数的值。而在第二次循环里，一半的情况下 j 为奇数的值将会被选到，但这种情况还是很容易被计算的。我们只需要简单地计算 $\text{SHA-256}(V[j-1])$ ，因为 $V[j-1]$ 在我们的缓存里。[\[3\]](#)在一半的时间内会产生这种情况，所以它增加了 $N/2$ 个额外的SHA-256计算。

因此，对内存要求量的减半只会增加 $1/4$ 的SHA-256计算量（从 $2N$ 到 $5N/2$ ）。总体来说，我们可以储存缓存区域 V 里的每个 k 排数据，即使用 N/k 的内存和计算 $(k+3) N/2$ 次的SHA-256迭代计算。在这个限制下，如果我们设定 $k=N$ ，我们就回到先前运算时间为 $O(N^2)$ 的计算。这些数字不一定非常精确地适用于Scrypt算法本身，但是渐近预测的方式确实是适用的。

除此之外，还有其他的设计可以弱化用时间来换取内存的能力。举例来说，如果一个缓存持续地在第二次循环中被更新，它可以让时间与内存之间的互换不是那么有效，因为这些更新必须被储存在内存中。

校验成本

Scrypt的另一个局限性是，它需要用与计算所用的同样大小的内存来做校验。为了让内存刚性有意义， N 需要变得比较大。这意味着一个Scrypt的计算要比一个SHA-256的迭代计算（在比特币里只需要一个

SHA-256计算就可以校验）昂贵许多倍。

这会产生负面的结果，因为在网络里的每个用户必须重复这个计算来检查每一个新发现的区块是否有效。这会减缓新区块传播和被认可的速度，从而增加了分叉攻击^[4]的风险。它还要求每个客户端（即使是轻量级的SPV客户端）拥有足够的内存来有效地进行函数计算。这样一来，实际上在加密数字货币中能够被Script用到的内存N是有限的。

一直到最近我们都不明确，是否有可能设计一个挖矿解谜程序在计算上是刚性内存类的，又可以很快地（不需要大量内存）进行校验。这个特性对密码进行哈希运算没有多大作用，在用于加密数字货币之前，这是Script算法的主要用途。

在2014年，一个叫作杜鹃鸟周期的新解谜算法被约翰·特龙普（John Tromp）所提出（起这个名字是因为这个算法的特性与杜鹃鸟的特性类似，杜鹃占巢）。杜鹃鸟周期算法，是从杜鹃鸟哈希表所衍生的一张图中寻找周期的难度而设定的，杜鹃鸟哈希表这种数据结构在2001年才被首次提出。除了建立起一个很大的哈希表之外，没有其他已知的方法来计算这个周期，结果却可以通过发现一个周期（相对小的）来简单地验证。

这个算法可能会让刚性内存或是内存限制类的证明工作在比特币共识里变得更加实用。可惜的是，这个函数无法在数学上证明，如果它不用内存的话就不能被有效地计算。通常，一个新的密码学算法看起来都是安全的，但是社区会对它持有保留意见，直到它存在了多年而没有被破解过。因为这个缘故，并且因为它也是最近才被发明的，当前杜鹃鸟周期算法还没有被任何加密数字货币所采用。

实际应用中的Script

Scrypt被许多种加密数字货币所使用，包括莱特币在内的几种热门币，结果好坏参半。针对莱特币Scrypt算法参数的ASIC已经存在（然后被其他几种另类币所复制）。令人惊讶的是，相较于大众电脑，这些ASIC在算力上的提高比起SHA-256相对普通电脑的提高，至少旗鼓相当甚至要更大！所以，Scrypt最终还是无法反ASIC，至少在莱特币上是如此。莱特币的设计者起初宣称反ASIC是莱特币的一大优势。但现在他们已经收回了这个说法。

这可能是莱特币所用的数值N（内存使用参数）比较低所造成的，它只要求128KB就可以进行计算（如果使用时间内存互换的模式，可能所需要的内存更低，这也被普遍用于GPU以获得更快的缓存）。低数值N使设计一个不需要复杂的内存存储总线的轻量级挖矿ASIC变得很容易，通常这种复杂的总线是读取十亿字节（Gigabytes）级别的随机存取存储器所需要的，而这些通用电脑都具备。莱特币的开发者没有选择一个比较高的内存参数（这会使ASIC更加难以设计），因为他们认为高内存参数所导致的高成本的校验过程是不太现实的。

其他抵抗ASIC的方法

请回忆一下，我们的初衷是想让可以大幅度提升计算性能的ASIC的开发变得困难。刚性内存解谜只是其中一个方法，还有其它方法。

遗憾的是，其他的方法都不是很科学，并且没有作为刚性内存函数而被设计过或者攻击过。最有名的一个叫作X11，其实就是把11个不同的哈希函数结合在一起，被一个叫作“黑暗币”(Dark Coin)的另类币所用（后面这个另类币改名叫DASH），在DASH之后也被其他一些另类币所使用。X11的目的是使设计一个有效的ASIC变得十分复杂，因为所有的11个函数的计算模块都要在芯片上被实施。但这其实对硬件设计者来说，也不过是一个小小的不方便而已。如果有一个针对X11的ASIC诞

生，那么马上会废弃掉X11的CPU和GPU挖矿。



X11的哈希函数出自何处？

从2007年至2012年，美国国家标准委员会组织了一个竞赛，这个竞赛选取新的哈希函数家族来作为SHA-3的标准，大量包含了设计文档和源代码的哈希函数作为候选方案被提交。虽然有很多候选方案在竞赛中被证实并不符合密码学安全规范，但其中有24个哈希函数经受住了所有已知的密码学攻击，X11选择了其中的11种，包括获得最终胜利的Keccak^[5]

另外被提出但还没有被实施的一个方法是使用一个移动的目标值来作为挖矿解谜。也就是说，解谜算法本身就会变化，就像比特币里的难度会周期性地改变一样。在理想的状态下，为上一个解谜算法而被优化过的挖矿硬件，对下一个解谜算法不再适用。我们不是很清楚要多久改变一次解谜算法，才能达到我们需要的安全要求。如果这是由另类币的开发者所决定的，这可能就变成了一种不可接受的中心化来源。比如，开发者可以根据他们已经开发出来的一种硬件（或者只是优化过的FPGA），去设计一个相对应新的解谜算法，他们自然就有了针对这个新算法的早期优势。

或许这些解密算法的顺序能够被自动生成，但这看上去也很难。一个想法是选择一大堆哈希函数（比如24个没有被攻破的基于SHA-3的算法），然后每个用上6个月到一年，在这么短的周期里很难开发新的硬件。当然如果这个顺序安排被事先知道，相应的硬件设计就可以按照函数使用的时间表来进行。

ASIC的蜜月

目前市面上还没有针对X11的ASIC面世，即便都清楚这种芯片的生产是可能的，这种现象显示了可能很有用的规律。因为适用X11算法的另类币的市值都不高，简单来说，还没有足够的市场价值吸引人去设计和生产针对X11的ASIC。一般来说，设计ASIC的前期投入都很高（不管是时间还是资金），同时生产单个硬件的利润相对来说比较低。因此，对于新的还没有被证实的加密数字货币，是不值得去投资研发针对性的ASIC，因为在新的硬件设备可用之前这个货币就可能失败了。即使有一个明显的市场需求，也会有硬件研发生产到出货的延迟。第一批比特币的ASIC从最初设计到最终出货花了近一年时间，这在硬件行业里已经算是很快了。

正因为如此，任何使用新的挖矿解谜算法的另类币都会经历一个ASIC蜜月期，在这段时间内，用GPU和FGPA挖矿(或许CPU挖掘)的利润会比较高。对于永久阻止ASIC的浪潮不太可能，但是吸引个人参与挖矿（并且因此而获得新币）的做法，在新币还处于步步为营的阶段，还是有价值的。

对于抵抗ASIC的争论

我们已经可以看到，从长远来讲做到反ASIC是不太可能的。但是也有一些其他意见，觉得从已经被证明的SHA-256解谜算法转变为一个密码学角度偏弱的新解谜算法，会存在一定的风险。甚者，SHA-256的挖矿ASIC已经接近当今硬件效能的极限了。这意味着，ASIC所带来的指数型增长可能结束了，之后SHA-256挖矿也会因此给网络带来最大的稳定性。

最后，还有一种意见认为，在短期内反ASIC也不好。在第3章中，

我们曾探讨过即使一个拥有全网51%算力的矿工，他如若尝试做出很多类型的攻击，也并不理性。因为这样一来会使币值汇率崩溃，使得矿工在挖矿设备上的巨额投资大幅减值，他通过挖掘赚来的比特币的价值也会大幅下降。

对于一个高度反ASIC的解谜算法，这个安全性的说辞可能会站不住脚。举例来说，一个攻击者可能会暂时租用巨大算力〔比如像亚马逊（Amazon）的EC2服务〕，用它来攻击，然后不会承受任何财务上的损失，因为他们不需要在攻击后继续租用这个服务。相比较而言，对于一个“对ASIC友好”的解谜算法，攻击者就不得不控制一大堆只可以用作加密货币挖矿的ASIC。这样的攻击者其实应该是看好比特币未来的发展，做了一个最大限度的投资。按照这个逻辑进行推理的话，为了最大限度地保护安全，或许挖矿解谜算法应该被设计成不仅仅要让有效的挖矿ASIC被设计生产出来，更应该让那些ASIC除了用于加密货币的解谜运算之外，没有任何其他用途！

[1] 也就是花费更多去提高内存的效能，并不能以相同比例去提高解谜的效能。——译者注

[2] Scrypt是由著名的FreeBSD黑客Colin Percival为他的备份服务Tarsnap开发的。Scrypt不仅计算所需时间长，而且占用内存也多，使得并行计算多个摘要异常困难，因此利用rainbow table进行暴力攻击更加困难。Scrypt没有在生产环境中大规模应用，并且缺乏仔细的审察和广泛的函数库支持。——译者注

[3] j是奇数时，减1为偶数，我们存的是有偶数的值的。——译者注

[4] 有关分叉攻击的内容，可以参见本书第5章。——译者注

[5] Keccak算法为SHA-3的一种加密标准。——译者注。

8.3 有效工作量证明

在第5章，我们讨论了比特币挖矿的能量消耗（有些人会说是浪费）是个潜在问题，经济学家称之为负外部性。我们估计比特币挖矿要消耗几十万千瓦的电能。所以一个明显的问题是，这些用来解谜运算的工作量是否对社会有所贡献？这其实是一个资源再生循环的问题，也会增加社会对加密数字货币的政策支持。当然，这个解谜算法也必须满足几个基本的要求，才能够在一个共识协议里被使用。

以前的分布式计算项目

在比特币诞生好多年之前，就有利用空闲的电脑〔或者叫“空闲周期”（spare cycle）〕来做一些其他工作的想法。表8.1列出了最受欢迎的几个志愿者运算项目。所有这些项目都有一个特性，使得它们适合成为解谜算法的运算。具体来说，它们需要解决的都是一种“大海捞针”型的问题，可能的答案存在于一个非常大的空间（或者说范围），搜索空间的每一小部分都可以进行并行的快速验证。最有名的例子是在SETI@home网站上，志愿者们被分配一小段无线电信号，用闲置的个人电脑来分析这段信号可能存在的模式以寻找外星文明，同时分布式计算网站（distributed.net）的志愿者被分配一小段可能的私钥来进行验证。^[1]

志愿者运算项目，成功地把一个很大的计算任务拆分成小份的任务，然后分配给每一个志愿者进行运算检查。事实上，这种模式在一个特别的叫作伯克利开放式网络计算平台（Berkeley Open Infrastructure for Network Computing，简称BOINC）上是很普遍的，这个平台被开发出

来就是用来给不同的个体分发小份额计算工作的。

在这些应用里，志愿者们主要都是被解决某个问题的兴趣所吸引，即使这些项目通常也会设立一个排行榜来让人们炫耀他们所贡献的算力。排行榜也导致一些人在自己的工作量上作弊，有一些被报告的工作量其实并没有实际完成，这也使得有些项目再分配一些额外的工作去检查网络上的这种作弊行为。金钱，是加密数字货币分布式计算应用的动力，只要技术上是可能的，一定会有参与者尝试去作弊。

表8.1 热门的志愿者运算项目

项目	成立时间	目标	影响
Great Internet Mersenne Prime Search	1996 年	找到大的梅森质数	连续 12 次发现最大的质数包括 $2^{57885161} - 1$
distributed. net	1997 年	密码学的暴力破解演示	首次公开成功地暴力破解了 64 位的密码私钥
SETI@ home	1999 年	寻找外星人	迄今为止最大的分布式计算项目，有 500 万以上的参与者
Folding@ home	2000 年	蛋白质折叠模拟在原子级别上的实现	史上最大算力的志愿者运算项目，超过 118 篇科技论文被发表

有效工作量证明的挑战

有了这些成功的项目，我们可以尝试简单直接地利用这些解决问题的成功方法。例如，在SETI@home的项目中，志愿者们被分配一小段无线电信号监听去寻找外星人，我们可以判断，外星人存在的概率，要比解谜算法找到“获胜”答案并且允许找到答案的矿工去创建一个区块的概率小很多。

但这个想法有几个问题。首先，并不是所找到的答案都有同样的概

率成为“获胜”的答案。参与者可能会意识到有特定区域会有更高概率找到异类，那么参与者就会有倾向性，只针对一些能产生不同寻常结果的区域进行分析。对于一个中心化的项目来说，参与者被分配工作，所以所有的区域最终都会被分析（当然对最有希望的区域会予以优先考量）。对于挖矿来说，任何矿工可以随意尝试任何区块，所以矿工会先涌向最有希望的区块。如果更快的矿工知道他们可以先尝试最有希望的区块，这就意味着解谜算法可能不是一个过程无关的算法。比特币的解谜算法与之相比就有不同，比特币的解谜算法中用来产生一个有效区块的临时随机数都是完全平等的，所以所有矿工都会随意选择一个临时随机数去尝试。这个问题展示了我们之前都已经习以为常的比特币解谜算法的一个主要特征：一个机会均等的解谜区域。

其次，考虑到SETI@home项目中存在着固定的数据量需要被分析的问题，这些数据基于射电望远镜（radio telescope）的观察。随着挖矿算力的不断增长，有可能某一天就没有需要加工的数据了。比特币在这方面也有不同，比特币算法有无限的SHA-256解谜可以被创造出来，这就说明了另一个重要的特征需求：永不枯竭的解谜库。

最后，考虑到SETI@home的项目中，有一个受信任的中心化的管理机构，负责发现新的无线电信号并判断志愿者们应该研究的内容。同样，由于我们使用解谜算法来构建一个共识机制算法，不可能假设一个中心化的机构来管理所有的解谜，这样我们就需要所有解谜的最后一个特征：通过算法自动生成。

哪种志愿者运算项目可能适合解谜算法

回到表8.1，我们可以清楚地看到，像SETI@home和Folding@home这样的项目不太适合去中心化的共识机制协议，两者都被证明了缺乏我们所列出的上述三个特性。distributed.net上的暴力破解密码学项目可能

适用，虽然它们通常被某些公司用来做某种加密算法的安全评估，但是不能通过算法自动生成。我们可以通过算法自动生成被暴力破解的加密方法，但是某种程度上这就是SHA-256不完全原像（partial preimage）算法已经做过的事，并且它没有任何有益的功能。

那就只剩下互联网梅森质数大搜索(Great Internet Mersenne Prime Search, 简称GIMPS)项目了，这个最具备可用性。这个办法的挑战是通过算法自动生成（找到下一个比当前最大质数更大的质数），以及谜底空间是不可穷尽的。事实上，质数的寻找确实是无穷的，因为质数的个数已经被证明是无限个的（特别是梅森质数是无限量的）。

梅森质数方法的唯一缺点，是需要花费很长的时间来寻找梅森质数，并且梅森质数非常罕见，事实上在过去18年里，梅森质数大搜索项目一共才发现了14个梅森质数，显然在区块链上每年才增加不足一个区块是不可行的。这个问题看起来是缺乏可调节的难度特性，我们在8.1节讨论过这个特性是非常关键的。无论如何，类似于寻找质数这样的解谜算法，看起来是可行的。

质数币

到2015年为止，唯一在实际中被应用的被证明具有有效工作的系统是质数币（Primecoin）。质数币的主要挑战是为质数找到一个“坎宁安链”（Cunningham chain）。坎宁安链是指 k 个质数的序列 P_1, P_2, \dots, P_k ，以使得 $P_k = 2P_{i-1} + 1$ 。也就是说，你选一个质数，然后把这个质数乘以2再加1以得到下一个质数，直到你得到一个和数（非质数）。含有2, 5, 11, 23, 47就是一个长度为5的坎宁安链，按照这个规则所获得的第六个数字95并不是质数（ $95 = 5 \times 19$ ）。最长的已知的坎宁安链的长度是19（从79, 910, 197, 721, 667, 870, 187, 016, 101开始），有一个被推测以及被广泛认可但没有被证明过的理论认为，存在一条任意的长

度为 k 的坎宁安链。

现在，要把这个理论变成一个可计算的解谜算法，我们需要三个关键的参数 m 、 n 和 k ，稍后我们会具体解释。对于给定的一个解谜挑战 x （上一个区块的哈希函数值），我们选择 x 上的前 m 位数。我们可以认为任何长度为 k 的链或者大于 k 的答案是正确的，这条链上的第一个质数是一个 n 位质数并且和 x 一样有 m 位的首段数据（ $n \geq m$ ）。值得注意的是，我们可以调整 n 和 k 的值，来让这个解谜变得更加困难。增加 k 的值（需要的链的长度）使得问题难度指数型增长，而增加 n 的值（链上的第一个质数的长度）使得问题难度线性增长，这就可以让我们对问题难度进行微调。其中， m 的值只需要足够大，使得在知道前一个区块的值之前的预先计算方法变得没有意义。

其他我们所讨论的属性看起来已经都有了：结果可以很快被校验，问题本身是无关过程的，题库可以无限大（假设对质数分布的知名数学推导是正确的），然后解谜可以通过算法做到自动生成。实际上，这个解谜算法已经被质数币用了两年，并且对许多给定的 k 值产生了坎宁安链里最大的质数。质数币还做了进一步的扩展，在其工作量证明中涵盖了其他类似的质数链，包括“第二”坎宁安链，其中 $P_i = 2P_{i-1}$ 。

这验证了在某些限定的情况下，有效工作量证明是具有实际运用的。当然，寻找大的坎宁安链有用与否，是有争议的。坎宁安链当然也代表了我们已知数学知识宝库的一小部分，其在未来可能会有一些应用场景，但在目前还没有实际的应用出现。

永久币和存储量证明

另外一种有效工作量证明叫存储量证明（proof of storage），也被称为可恢复性证明（proof of retrievability）。不同于需要一个单独计算

的解谜算法，我们可以设计一个需要存储大量数据被运算的解谜算法，如果这个数据是有用的，那么矿工在挖矿硬件设备上的投资就可以被用于大范围分布式存储和归档系统。

让我们看一下永久币（Permacoin），这是第一个用于共识机制的存储量证明方案。首先我们讨论一个大文件 F ，我们假设所有人都认可 F 的价值并且这个文件不会被改变。例如，当一个加密数字货币上线时，由一个可信任的分发者选择 F ，这有点类似于任何一个加密数字货币启动时都需要一个创世区块，理想状况下这个文件会具备公共价值。例如，大型强子碰撞(Large Hadron Collider, 简称LHC)的实验数据，这个数据已经达到了几百拍字节（petabytes, 用PB表示）的大小，对这些数据的备份是很有价值的。

当然，因为 F 存储量非常巨大，大多数参与者都无法对整个文件进行存储，但我们已经知道，在不需要了解整个文件的情况下，如何使用密码学里的哈希函数来确保每个人都对 F 认可。最简单的方法是，每个人都认可 $H(F)$ ，但更好的方法是用一个大型梅克尔树来代表 F ，所有的参与者都认可梅克尔树的根值。现在，每个人都认可 F 的价值，证明 F 的任意一部分是正确的就变得很有效率。

在永久币系统中，每一个矿工 M 存储着任意 F 文件的子集 $F_M \subseteq F$ 。为了实现这一点，当矿工产生一个公钥 K_M 来接受资金时候，他们就对该公钥进行哈希运算以生成一个区块 F_M 的虚拟随机数集，他们必须存储这个数集以实现挖矿的目的。这个子集就会变成某个固定数量的区块 k_1 的一部分，我们必须在这里做一个假设，当矿工开始挖矿的时候，他们有能力获得这些区块——可能是从一个标准文件源地址下载下来（见图8.2）。

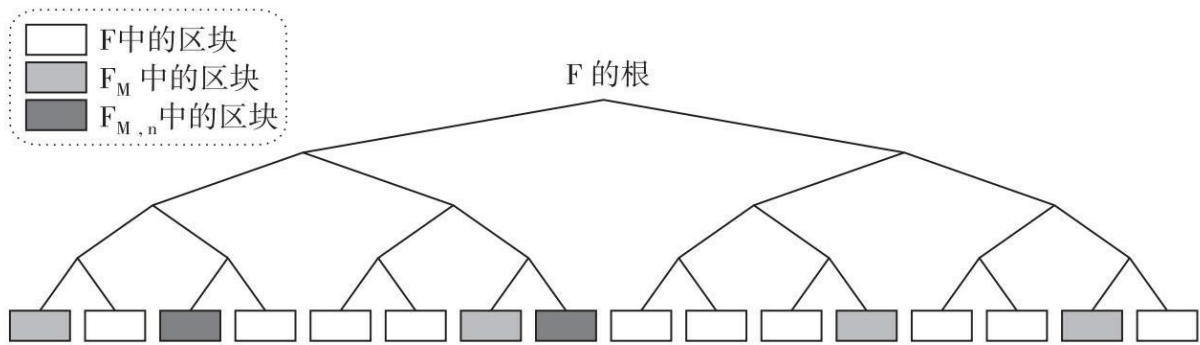


图8.2 在永久币系统中选择一个文件的随机区块
注：在这个案例中， $k_1=6$ ， $k_2=2$ 。在实际应用中，这些参数会大很多。

一旦矿工在本地存储了 F_M ，这个解谜算法就非常类似于传统的SHA-256挖矿了。给定前一个区块的哈希值 x 时，矿工选择一个临时随机数 n ，将其进行哈希运算并产生一个虚拟随机数子集 $F_{M,n} \subseteq F_M$ ，这个子集包含了 $k_2 < k_1$ 个区块。值得注意的是，这个子集是由所选的临时随机数和矿工的公钥共同产生的。最后，矿工对 n 以及 F_k 中的区块，进行SHA-256的哈希函数运算，如果计算的结果是低于目标难度的，那么也就意味着他们找到了一个有效的方案。

校验一个解谜算法的结果需要以下几个步骤：

- 校验 $F_{M,n}$ 是由矿工的公钥 K_M 和临时随机数 n 共同产生的。
- 通过检验其在梅克尔树节点到全局统一的树根路径，来检验 $F_{M,n}$ 中的每一个区块是正确的。
- 校验 $H(F_{M,n} \parallel n)$ 的值比目标难度要小。

我们很容易看出，为什么解谜过程需要矿工在本地存储所有的 $F_{M,n}$ 。对于每一个临时随机数，矿工都需要计算 $F_{M,n}$ 中随机子集的哈希值，如果通过远程访问一个存储空间来获取文件，就会非常慢，几乎不可能实行。

不同于Scrypt算法的案例，如果 k_2 足够大，并没有一种可行的类似于时间内存的权衡方案。如果矿工仅仅在本地存储了一半的 F_M ，并且 $k_2=20$ ，那么在他们找到一个不需要从网络中取回任何文件区块的临时随机数之前，他们必须要尝试100万次，降低一定量的存储负担会以计算量指数型增长为代价。当然，由于 k_2 梅克尔树路径要在所有的路径中被传输和校验，如果 k_2 设得太大，也会使运算变得非常低效。

k_1 的设定也可以有所权衡。更小的 k_1 意味着矿工需要更少的本地存储空间，因此这种挖矿就更加民主化（更多的人可以参与）。然而，这也意味着，大量的矿工即使有能力提供更大的存储空间，他们也没有动力去存储多于 k_1 个F区块。

同样，这是一个对完整的永久币做了细微简化的方案，但是对我们理解整个设计的关键部分来说是足够的了。最大的应用挑战，当然是找到一个合适的大文件，这个文件要有一定的重要意义，同时也是公共的，需要保存多个备份。如果F文件本身随着时间的推移会发生变化，或者随着时间的变化而调整难度，这样会使方案变得更加复杂。

长期的挑战和经济意义

总结一下本节内容，有效工作量证明是一个非常自然的目标。考虑到一个好的共识机制所需要的其他解谜算法，实行起来也有相当大的挑战。即使如此，至少本文所举的两个案例——质数币和永久币——在技术上是可行的，虽然它们也都有一些技术方面的缺陷（主要都是需要更长的时间去验证解谜结果）。此外，对比在比特币挖矿中动辄数百万美元的投入以及大量电力的消耗，这两种加密数字货币的应用都对社会公益有一些贡献。

有效工作量证明是否应该是纯公益的，有一个有趣的经济学方面的

争议。在经济学中，公益的意思是非排他性的，也就是说所有人都可以参与使用，并且是非竞争性的，对公益的其他用途不应该影响其本身的价值。一个经典的例子就是灯塔。

我们这里所讨论的案例，比如蛋白质折叠（protein folding）^[2]，就不是一个纯公益的项目，因为有一些公司（比如大的制药公司）可以从中获利。实质上，这些机构挖矿的成本会相对变低，因为它们可以获取其他人无法获得的额外利益。

^[1] 大约有500万人参加这个计划，包括译者本人。——译者注

^[2] 蛋白质折叠问题被列为“21世纪的生物物理学”的重要课题，它是分子生物学中心法则尚未解决的一个重大生物学问题。——译者注

8.4 不能外包的解谜算法

我们现在再看一下对于替代挖矿解谜的另一个设计重点：防止矿池的产生。我们在先前的第5章里谈到，大部分的比特币矿工都会加入一个矿池，而不是独立挖矿。这就造成了少量矿池拥有绝大部分挖矿算力的现象。由于每个矿池都有一个中心化的管理方，有些人担心这其实违反了比特币去中心化的核心设计原则，会危害到比特币的安全性。

拥有大部分算力的矿池显然是一个问题，任何一个中心化管理的矿池可能会实施一套自定义的挖矿策略，然后用它来攻击网络。这种矿池也是黑客们攻击的目标，因为通过攻击矿池可以迅速地控制大量的挖矿算力。矿池管理员也可能会删改交易或是强迫收取更高的交易费。矿池中拥有大多数矿工，意味着大部分矿工都没有运行一个完全有效节点。

有意思的是，这些担忧有着现实世界的影子，比如选票。在美国和其他许多国家，出售选票是非法的。加入一个被一方控制的矿池，和在比特币的共识协议里出售你的选票有点类似。

矿池的技术要求

回忆起来，矿池看起来是一个突然发生的现象。并没有证据显示，中本聪在比特币的最初设计中考虑过矿池的概念。在互相不信任的个体之间运行一个有效率的矿池，这样的事情在最初的几年里看起来不太现实。

正如我们在第5章所看到的，矿池通常会指定一个管理员，他有一个大家都知道的公钥。每一个加入的矿工还是按照往常一样进行挖矿，

然后递交“近似”或者“部分”答案给矿池管理员，这些答案在低级别难度的时候可能就是一个有效答案，通过这种做法来证明他们做了多少工作量。当矿池中的某一个参与者找到了一个有效区块的时候，这个管理员会按照每个人所提交的工作量的占比来分配奖励。虽然有很多种不同的分配方式，但是所有矿池都遵循这个基本模式。

正因为如此，矿池的存在依赖于比特币的两大技术特征。第一，一个矿工很容易通过提交工分来证明（概率上）他所做的工作量。不管实际上找到一个有效区块是多么困难，通过设定一个足够低的合格工分的临界值，矿工可以容易地证明他们在任意精度的工作量。考虑到我们需要解谜题目可以在任意难度上被创造出来，这个问题看起来很难改变。

第二，矿池成员可以容易地向管理员证明，他们遵守规则并且通过实际运算来寻找有效区块，然后矿池会作为一个整体接受奖励。这是行得通的，因为这个矿池的公钥是被写进币基交易，并包括在区块里的梅克尔树上。即使一个矿工找到了一个有效区块，甚至只是一个近似区块（也叫工分），他也无法改变整个矿池的公钥，而成为新铸币的接受者。

“区块丢弃”攻击（block-discarding attack）

矿池的这种设计有一个弱点：没有办法来确保矿工在找到有效区块的时候一定会提交给管理员。假设有一个矿池成员对一个大型矿池不满，他可以正常地参与挖矿然后提交工分，但他在找到一个有效区块（可以让整个矿池获得奖励）的时候，并没有告诉管理员而是直接把它丢弃掉。

这个攻击降低了整个矿池的挖矿能力，因为攻击者的工作量并没有实际贡献到挖矿中去。但是这个矿工依然会收到奖励，因为他看起来也

在不断地提交工分，只是运气不好没有找到有效的区块。如果这个矿池的奖励设计方案是收入中性的（也就是所有的挖矿奖励都被分发到每个参与者），那样的话这个攻击会让这个矿池亏损。

这种攻击被称作民间攻击或者是蓄意破坏攻击，这也被认为是一种蓄意破坏，因为这个攻击看上去对攻击者和矿池都是不经济的、代价不菲的。这个攻击者本身也会遭受损失，因为他所丢弃的有效区块将会使他放弃他应该有的一部分奖励回报。当然，这个攻击者还是会由于其他一些挖矿解密算法而获利。

看起来一个理性的矿工不会采用这种策略，因为他会有所损失而不会得到任何实际的回报。但（令人惊讶的是）在某些情况下，这个策略是可以有利可图的，我们在下文有所讨论。但是无论如何，我们想要设计一个全新的挖矿解谜算法，以确保这种策略永远都是有利可图的（以抵抗矿池的存在）。



矿池之间的区块丢弃攻击

好多年以来，人们都觉得进行区块丢弃攻击是无利可图的，实际上如果两个矿池之间的互相攻击却不一样。这种方案已经被提出来好多次，伊泰·艾瑞尔（Ittay Eyal）2015年的论文中首次深入分析了这种攻击模式。

我们考虑一个简单的案例：假设两个矿池A和B，每个有50%的全部挖矿算力。现在假设B动用了一半的能力（25%的总体算力）来加入矿池A挖矿，然后把所有找到的有效区块丢弃掉。我们可以推演，在一个简单的模型里，B会赢得5/9的所有奖励，大于他正常挖矿时候所获得的50%的奖励。在这个简单的案例里，动用一半的挖矿算力去攻击矿池A对矿池B来说是一个最佳的策略。

这个案例随着矿池数量的增加而变得更加复杂。截至本书撰写之时，丢弃区块攻击在实际中还没有被大范围观察到。但长期来看可能性还是存在的，像这类攻击会对大型矿池的运营产生关键影响。

奖励破坏

我们设计这种攻击的目的，是让矿工们即使加入了一个矿池挖矿，也会缺乏向矿池管理员提交有效区块的动力。目前，只有矿池管理员可以获得挖矿奖励，因为管理员要求所有的参与者在他们挖矿的币基交易中加入一把特殊的公钥。这个公钥是否被正确地放入，可以在提交近似区块的时候被很容易地检查验证。矿池管理员是唯一知道私钥的人，因此可以决定新铸币的走向。

但如果我们要求所有的参与者都知道私钥（这样一来，当找到有效区块的时候大家都可以重新定义区块奖励的去向）呢？为了做到这一点，我们需要一个解谜算法，每一个解谜运算的尝试都要求知道币基交易里的私钥。我们可以把解谜从“找到一个区块，其哈希值低于一个特定的目标”改成“找到一个区块，这个区块里的数字签名的哈希值低于一个特定的目标”。这个数字签名必须要用币基交易里同一把公钥来计算。

这样的解谜算法，会给矿池管理员两个都不可靠的选择：他们可以把私钥分发给所有成员，如此，他们之中任何一人都可以私自挪用全部矿池资金。另外一个办法是他们可以代表矿池成员进行签名。计算一个签名的计算量比计算一个哈希函数要大许多，这样一来，矿池管理员会承担主要的苦活与累活，所以最好让矿池管理员成为一个独立的矿工。

不能被外包的挖矿的优劣

由于这类解谜算法不能够有效地（并不是完全不可能）被外包到一个不能被信任的参与者，这就使得成立一个由不被信任的参与者所组成的矿池变得十分困难。它可以有效地阻止所有的矿池形成，即便是像P2Pool这样成立一个没有矿池管理员的去中心化矿池。

存在如下争议，部署这类解谜算法可能会不可抑制地造成更多的中心化，而不是更少。因为概率上较高幅度波动（找到有效区块而获得奖励的概率问题）会让小矿工们不敢参与挖矿，剩下的只会是大型挖矿团队。目前，虽然矿池表面上控制了大量的挖矿算力，但还是不清楚如果他们想利用这个优势来发起攻击的话，其中许多成员是否会叛逃。大型挖矿矿池和可以承受高幅度收入波动的小矿池，到底哪个风险更大？这是一个未能解决的问题。

设计一个共识协议，理想方案是小额度地奖励每个找到低等难度解谜答案的矿工，以“自然地”降低概率波动风险。这就意味着矿工们不需要组成矿池，同时小矿工们还可以参与挖矿获利。仅仅降低每个区块产生之间的时间间隔不会起到作用——它需要被降低1 000倍或者更多，才能够在概率风险上与大型挖矿矿池所面临的情况相当。但到那个时候，每个区块之间的间隔只有不到一秒，陈旧区块的数量会变得不可控制的高。还有一个问题，是否存在另一种共识协议，可以做到在不需要瞬时广播所有解谜结果的情况下，让解谜运算变得更加容易？

8.5 权益证明和虚拟挖矿

在结束本章之前，我们讨论一下这个想法：用虚拟挖矿（virtual mining）来替代算力挖矿。虚拟挖矿是指一组不同的挖矿方法但它们都有一个共同的特点——对参与的矿工只要求少量的计算资源。

建立一个封闭挖矿系统

作为一个思想实验，假设比特币或是其他加密数字货币成为全球主要支付手段。矿工起初会拥有一些加密数字货币来购买挖矿设备和支付电耗，以此获取一些新币来作为挖矿的奖励（见图8.3）。这基本上是个消耗资源的过程。

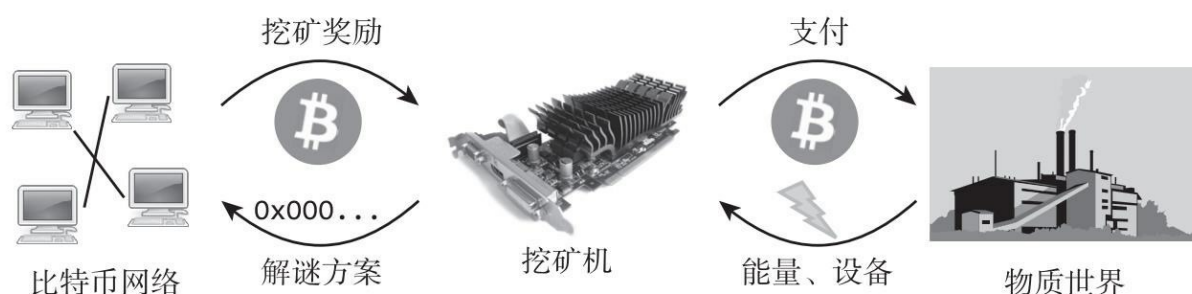


图8.3 比特币挖矿的资源循环

一旦挖矿设备变成了一种商品，并且电力也是一种商品（本来就是），没有矿工有任何优势可以更有效地把他们起初拥有的加密数字货币转化成挖矿奖励。除非有细微的效能差距，挖矿投入最多的矿工将会获得最大的挖矿奖励。

推动虚拟挖矿的基本问题是：如果我们把挖矿设备和能耗这一环节省去，会产生什么结果？毕竟，这个过程主要是用来证明谁在挖矿这件

事情上投入最多。为什么不简单地把挖矿“算力”按比例分配给当前所有的持币人？

回忆一下比特币挖矿的初衷是在区块链上建立起一个投票机制，有更多算力的矿工会得到更多的投票权力。因此，我们可以设计一个“投票”系统，选票（投票权力）是由每个人所拥有的当前币量所决定的。

虚拟挖矿的优势

这个方法的优势是显而易见的：它把如图8.3中右边浪费资源的一半去掉了，留下了一个封闭的系统，如图8.4所示。



图8.4 虚拟挖矿的资源循环

除了简单化之外，这个方法会大大减少比特币对环境的影响。它不会把能耗降到零，因为矿工总是会消耗一些计算资源来和网络通信验证，有一些虚拟挖矿方案也要求少量的挖矿计算力。但总体上，比特币里绝大部分的挖矿工作量可以被省去。

虚拟挖矿还可以阻止中心化的发展趋势。因为没有硬件，所以也不

必担忧有ASIC的问题。每一个矿工挖矿的效率都和其他人完全一样。任何虚拟矿机所用的解谜算法都是反ASIC的。

这可能是虚拟挖矿最重要的一点。虚拟挖矿可能解决了我们在讨论反ASIC解谜算法时候所遇到的问题，也就是考虑到货币的长期健康，矿工可能不会去投资挖矿设备的生产。任何一个比特币的持有人其实也是这个货币的利益相关者，一个强大的虚拟矿工（比如持有51%或更多的币）是一个非常大的利益相关者。他们有原动力来做对整个系统有利的事，因为这样一来他们所持有的币也会增值。这比“矿工已经投入了大量的挖矿设备，且设备价值会基于未来的币值，所以没有人会进行恶意行为”的说法更有力。

这就是“权益证明”这个名字的来源。除了节省挖矿设备和节省能源之外，可能虚拟挖矿的最大动力，来自这个货币的利益相关者有着强烈的意愿成为这个系统的维护者。

实施虚拟挖矿:点点币

有许多种不同的虚拟挖矿，我们在这里只讨论最常见的几种。我们要强调的是，这些想法还没有被严格地用科学的方法研究过，也没有像比特币的工作量证明一样因为比特币的普遍性而经过实战洗礼。

我们先看一下在2012年启动的**点点币**（Peercoin），是第一个使用权益证明的另类币。点点币是工作量证明与权益证明的一种混合体，“拥有量”以“币龄”为计价单位。一个特定的还没有被使用交易的输出的币龄，是“这个输出里的币量”与“这个输出里还没有被使用过的区块数量”的乘积。现在，为了挖到一个区块，点点币的矿工也必须像比特币的矿工一样去进行一个SHA-256的解谜运算。但是，这个解谜运算的难度会随着他们想消耗多少币龄调整，消耗越少难度就越低。为了做

到这一点，这个区块包括一个特殊的“币拥有量交易”（coinstake transaction），在这个交易里，有些交易被用掉只是为了把它们币龄重设成零。这些在币拥有量交易中被消耗的币龄总和，决定了工作量证明解谜运算中发现一个有效区块的难度。

矿工可以在最初用很大的计算力和一些很少的拥有量来挖矿，但是可以用公式来设定难度：当一些币龄被消耗后，找到有效区块会变得十分容易。这个运算型解谜的效果主要是为了保证，在有两个矿工尝试消耗同样大小币龄的情形下，这个过程仍然是随机的。

许多其他的虚拟挖矿另类币方案使用了略微不同的设计，包括Nxt、BitShares、BlackCoin和Reddcoin。在这些设计方案里，一定数量的币被消耗用于使运算型解谜变得极为简单，这使得解谜运算不再是挖矿过程中最主要的挑战。

权益的其他形式

有两种混合模式值得探讨：

- **权益证明。** 最简单的权益证明模式是使那些拥有大量币控制权的矿工挖矿更加容易。这类似于点点币的币量和币龄混合证明，只是在这个模式中不考虑币龄。这个模式的坏处是，不像点点币那样每次成功获得有效区块之后重置币龄，最有钱的参与者总是可以最容易地挖矿。

- **储量证明。** 在这个模式里，当一个矿工用一些货币来铸造一个区块的时候，这些货币针对一定数量的区块被冻结。这可以被想象成币龄的一个镜像：这个系统奖励那些希望在未来一段时间不消费的矿工，而不是那些在过去一段时间内不使用货币的矿工。在上述两种情况下，矿工的收入来自因为不能使用货币去做其他事

情的机会成本。

无利害关系问题

虚拟挖矿是科研的前沿领域，还有许多未解的问题。即使有一些加密数字货币已经启动并且使用了虚拟挖矿，它们都面临和比特币一样的压力，即防御有目的性的攻击者。

虚拟挖矿有一个常见的漏洞，被称为“无利害关系问题”（nothing-at-stake problem）或者“股权粉碎攻击”（stake-grinding attacks）。假设一个有着小于50%的币拥有量的攻击者，尝试制造一个有k个区块的分叉，如同我们在前面讨论过的，这样的分叉攻击有着相当高的失败概率。在传统挖矿里，一个失败的攻击有着很高的机会成本，因为矿工本可以在挖掘的过程中赚得奖励，而不是浪费挖掘资源在失败的攻击上。

但在虚拟挖矿里，这个机会成本并不存在。一个矿工可以既在当前最长的区块链上挖矿，同时又可以进行一个创建分叉的尝试。如果分叉成功，则会消耗掉大量的筹码；如果失败，这个失败的记录不会出现在最长的区块链上。因此，理性的矿工也会不断地尝试分叉攻击。

对于这个问题，有一些不同的解决办法。大多数的虚拟挖矿方案都积极地使用检查点来防御长分叉攻击。但是正如之前讨论过的，这有点和去中心化的共识协议概念背道而驰了。



分叉攻击和检查点

当你下载比特币核心钱包软件时，有几个硬编码的检查点，或者过去区块的拼接。这样做的根本目的是让首次下载区块链更加顺

利。如果没有检查点，其他节点可以使用伪造的（但有效的）区块和分支来冲击你。对于当今的攻击者来说，在低区块高度产生有效的谜题解决方案是非常简单的，那就是接近起源区块，因为初始阶段的难度相对较低。你最终会发现这些区块不在最长的有效分支上（更精确地来说，不在最高总体难度的有效分支上），但你必须浪费资源来做这件事情。

有些另类币，特别是虚拟挖矿计划，已经采取了以检查点作为防御分支攻击的强大形态。节点会从指定检查节点收到检查点的常规更新，该更新由指定的私钥签发。节点会放弃与检查点冲突的分支。这种机制使得检查点的运作方，尤其是另类币的创建者，能从分叉和“转回”区块中选择胜出者。这种设计非常有趣，但是已不是去中心化一致认可的协议。

以太坊（Ethereum，一个在2015年启动的另类币，我们将在第10章中详细讨论），建议了一个称为“Slasher”的方法来惩罚尝试进行分叉攻击的矿工。在Slasher方案中，使用筹码去挖矿需要用私钥对当前区块进行签名，来应对那些进行作弊的交易，如果矿工曾经使用相同的筹码去签署两个不连续的区块链（不是前后关系），Slasher允许其他矿工可以在区块链上输入这两个签名作为作弊的证据，并且拿走一部分筹码以作为奖励。虽然看起来这个方案非常有效，但是协议本身非常复杂，还没有被实际部署。

一个终极的防御攻击方式可能存在，就如同我们在传统挖矿方案中看到的，矿工可以简单地没有足够的动力去进行攻击，因为即使攻击成功，也会危害整个系统并使得他们所拥有的筹码贬值。

虚拟挖矿的其他弱点

虚拟挖矿还有其他两个弱点值得提及。第一，在某种形式的虚拟挖矿方案中，即使“股权粉碎攻击”不存在，也可能使得某些类型的攻击变得容易，因为挖矿“蓄力”（save up）是可能的。例如，大量的币可以被积蓄起来，直到可以进行一次剧烈的挖矿变化使得分叉成为可能。即使是某个类似于Slasher这样严禁同时在两个区块链上挖矿的系统上，也是可能的。为了防止这样的攻击，点点币限制了币龄参数不能超过90天。

第二，如果虚拟挖矿中的某个矿工获得了51%的筹码，他可以通过只在他的区块上挖矿的方式永远保持这个优势，基本上也就意味着可以控制整个区块链。如果有新的筹码和交易费从区块奖励中产生，那个拥有51%的矿工也会抢去这些奖励，这会让他的筹码慢慢接近100%。在传统挖矿模式中，即使有一个51%的矿工存在，永远可能存在拥有更大算力和更低能耗的其他矿工出现，并且会减少最大矿工的市场份额。在虚拟挖矿里，很难避免这个问题。

虚拟挖矿有可能真的成功吗

在比特币的主流社区里，虚拟挖矿是有争议的。有一个说法是，系统的安全性必须建立在真正的资源消耗上，也就是动用真正的电脑硬件和消耗电能去进行解谜运算。如果这个理论成立，工作量证明上的能源耗费可以被看成是系统的安全费用。但这个论点还没有被证明，就像虚拟挖矿的安全性也没有被证明一样。

总结来说，人们想改变比特币挖矿解谜算法的很多方面，这也是研究与创新的重点区域。到目前为止，还没有一个替代方案具备理论健全性和实用性。例如，即使Script算法在另类币中很受欢迎，但是也没有做到真正的反ASIC，而且其用途也还不清楚。当然，替代的解谜算法完全有可能在未来获得更大的成功。毕竟，比特币本身也经历了数十年的不断失败的尝试与发展，才最终成为一个既有很好的设计理念又有相

当的实用性的加密数字货币。

延伸阅读

定义刚性内存功能和建议范本的论文是：

Percival, Colin. “Stronger Key Derivation via Sequential Memory-Hard Functions,” 2009.

您可以通过如下网址阅读：

https://www.bsdcan.org/2009/schedule/attachments/87_scrypt.pdf.

关于内存范围（memory-bound）功能的早期论文包括：

Abadi, Martin, Mike Burrows, Mark Manasse, and Ted Wobber. “Moderately Hard, Memory-Bound Functions.” ACM Transactions on Internet Technology 5(2), 2005.

Dwork, Cynthia, Andrew Goldberg, and Moni Naor. “On Memory-Bound Functions for Fighting Spam.” In Advances in Cryptology—Crypto 2003 . Berlin: Springer, 2003.

关于Cuckoo Cycle proposal的研究包括：

Tromp, John. “Cuckoo Cycle: A Memory-Hard Proof-of-Work System.” IACR Cryptology ePrint Archive, 2014.

您可以通过以下网址阅读：

<https://eprint.iacr.org/2014/059.pdf>.

关于永久币的介绍请参阅：

Miller, Andrew, Ari Juels, Elaine Shi, Bryan Parno, and Justin Katz. “Permacoin: Repurposing Bitcoin Work for Data Preservation.” In Proceedings of the 2014 IEEE Symposium on Security and Privacy , 2014.

您可以通过如下网址阅读：

<http://research.microsoft.com/pubs/217984/permacoin.pdf>.

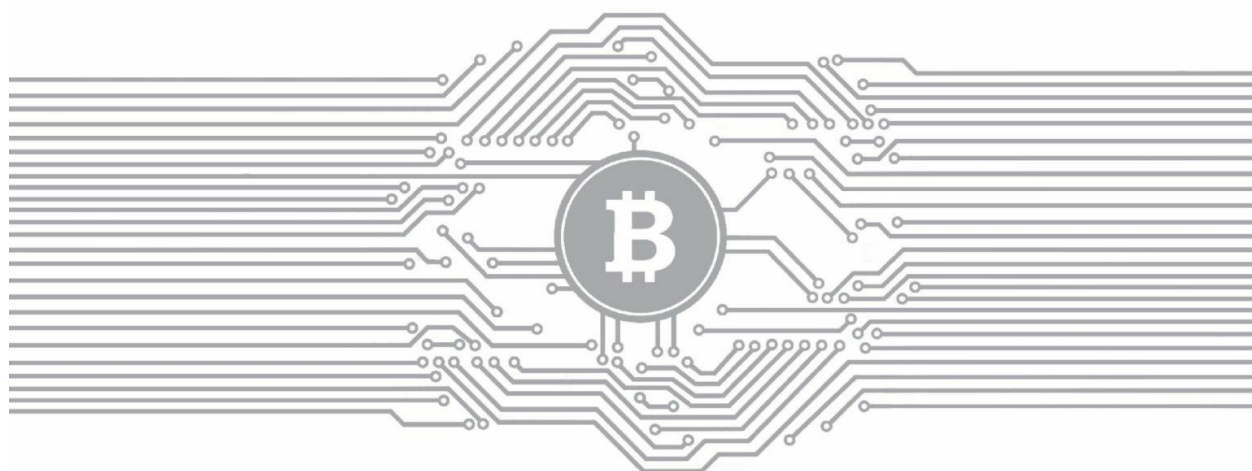
讨论不同的哈希函数和SHA-3竞争的论文是：

Preneel, Bart. “The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition.” In Topics in Cryptology—CT-RSA, 2010 . Berlin: Springer, 2010.

关于不可外包谜题的介绍是：

Miller, Andrew, Elaine Shi, Ahmed Kosba, and Jonathan Katz. “Nonoutsourcable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions.” In Proceedings of the 22nd ACM Conference on Computer and Communications Security , forthcoming.

第9章 比特币“平台”



在前面的章节里，我们展示了比特币的技术基础架构和它作为货币的机理。现在我们来探讨除了货币之外，比特币可以作为核心组成部分的其他应用。这些应用，有些是直接利用了比特币的当前特性，并未做任何修改，而更多的则是需要做一些微小调整的。

我们根据应用的实用性和学术上的趣味性选择了下述应用案例，尽管案例并不能穷举，但这些关于比特币运作的例子（或者设想中的运作模式），将给您对比特币新的用途看法带来一些启示。

9.1 比特币作为一个只能被添加的记录

比特币是一个只能添加而不能删除的记录。它是一种可以不断添加新的数据，但是数据一旦被添加上去，就变得不可修改并且永久保存的数据结构。因此，通过比特币，我们可以获得一个时间顺序：判断一个数据是在另一个数据之前还是之后被写进了记录的。这个次序是由区块之间的哈希函数指针，而不是区块上的时间戳所决定的，因为时间戳可以作假，或者是由于矿工更改时间戳的值使其变得更小（更早），或者是矿工的计算机时钟没有同步，更或者是由于网络延时产生的差异。话虽如此，如果一个区块的时间戳延迟了好几个小时，它就会被其他的矿工们拒绝。所以时间戳还是相对准确的。通过下面的示例，我们可以看到，这些特性是有实际用途的。

安全时间戳

比特币这种只能被添加的记录特性可以被用来建立一个**安全时间戳**（secure timestamping）系统。假如，想要证明在时间T我们就知道了x的值，但并不想披露它的具体值。只有在未来很长时间后，当有可能需要证明我们确实知道这个值的时候，才有可能需要去披露它（当然，如果我们在时间T知道x的值，我们在T之后的时间还是知道这个x的值）。而且我们一旦证明了这一点，就需要使这个证据具备永久性。

在第1章中我们看到，可以用哈希函数来锁定数据x。我们不需要公布x值本身，取而代之地，只需要在区块链里公布这个数据值的哈希函数 $H(x)$ ，即可以来证明我们知道这个X值。这个哈希函数的特性，保证了我们不可能再找到另外一个数据y，其哈希函数结果与x的哈希函数结

果一致，也就是说，当 $y \neq x$ 时， $H(x) = H(y)$ 是不存在的。我们还可以依赖哈希函数另外一个常用的特性：只要 x 本身具备比较高的**最小信息熵分布**特性（distribution with high min-entropy），也就是说， x 是不可预测的，那么 x 的哈希函数结果不会透露关于 x 的任何信息。如果 x 本身没有这种不可预测的特性，就像我们在第1章中探讨的，我们可以选择一个有较高的最小信息熵分布的随机数 r 和 x 组合签名，然后用 $H(r|x)$ 作为对外公布的一个数值约定。

这个设想的核心就是，我们在时间点 T 只向外公布哈希函数 $H(r|x)$ ，然后在之后的某个时间点来公布 r 和 x 。任何人看到这个只能做增量的记录，都会相信在我们发表 $H(r|x)$ 的时候我们一定知道 x ，因为没有除此之外的其他方法可以让我们产生那些数据。

时间戳的应用

这个安全时间戳到底有什么用途呢？一个可能的应用就是可以用来证明创意的优先性。假设我们想证明，申请专利的一些创意点子早就在我们头脑里存在。我们可以在产生创意的第一时间，就将设计文档或者示意图草稿在区块链里用哈希函数发表出来，但不会向任何人泄露这个创意的具体内容。之后，当我们提交专利申请或是公布这个想法的时候，我们可以将最初的设计文档和相关信息发表出来，任何人都可以查证这些文件的函数时间戳，来证实我们在这之前，也就是我们发布设计文档的哈希函数约定的时候，就已经有了这个创意（证明我们对这个创意的时间上优先所有权）。

我们还可以用同样的方法来证明，其他人收到过我们发给他们的信息。假设爱丽丝雇用鲍勃去做一个编程的工作——他们之间的合同规定，鲍勃必须在一定的时间内将他所做的工作内容提交给爱丽丝。双方都想要获得一个保证，如果将来对相关工作内容有争议，比如鲍勃是否

按时提交程序或者他提交的内容是否满足合同要求，双方都希望可以有相关的事实去证明。为了确保这一点，他们可以互相协商，将鲍勃提交的工作内容共同签名后，再在区块链上发表它的哈希函数。任何一方如果对提交的时间或者内容撒谎，另一方可以通过披露哈希函数的输入来重现当时发表的内容，来证明对方是错的（比如在法庭上）。

安全时间戳功能还有许多其他有意思的应用。有一种完全公钥签名方案，被称为盖伊·福克斯签名方案（Guy Fawkes signature scheme），相比较通常的公钥签名，只是利用了哈希函数和只能做增量记录的记录特性，而不需要任何重量级的加密算法。

对未来预测证明的攻击

我们目前无法仅仅用时间戳就证明对未来的准确预测，能对未来进行预测（clairvoyance），当然非常好。而且从表面上看，这好像可以做到。在一个事件发生之前（比如一个体育比赛或是选举）发表一个对结果的预言，然后在事件发生之后，再证明在之前就已经预测到了。但这个方法是否真正可行？

在2014年下半年的世界杯决赛阶段，有人想用这个办法来“证明”世界杯的组织方国际足联(Federation Internationale de Football Association, 简称FIFA)在搞腐败。当时有个推特账号，由于在一些重要比赛之前就可以准确地预测到这些比赛的结果，因而被广受关注。比如，该账号准确地预测到德国队会在加时赛取胜并且马里奥·格策（Mario Götze）会进球。这看起来可以证明，要么是微博主人有预知未来的能力，要么是比赛被操纵了。然而事实上，这个博主只是在比赛前发布了所有可能发生的事件，比如，对于所有的参赛球员，都有一条关于他会进球的微博，以及对于每一种可能的最终比分，都有一条相关的微博等（见图9.1），然后在比赛结束之前，博主删除了所有那些不准确的预测，只

留下那些准确的“预测”。



图9.1 试图对未来进行预测

注：这就是那个虚假的试图通过预测比赛结果来“证明”世界杯决赛圈的比赛被操控了的推特账号。其中第一个和第四个在赛后被证明是正确的，其他不准的预测就被删掉了。

可以用同样基础的攻击方法攻破任何安全时间戳系统。你只需要在

事先预埋下所有的结果，然后最终只披露那个正确的结果。这就意味着如果你想证明你有预测能力，就必须去证明你做且只做了一个预测结果，而不是多个预测。但如果你想基于哈希函数揭示结果，是很难实现的，尤其是在比特币的区块链上，因为安全时间戳系统并不将承诺与任何个人身份识别相关联。如果你不揭示它们，就会很容易公布很多种承诺，而那些你从未揭示的承诺很难轻易追溯到你。

过时的安全时间戳

这里介绍一个简单的低科技含量的安全时间戳方案：通过刊登广告，你可以在一份报纸或者其他媒体上登出你预测结果的哈希函数值，相关的旧报纸杂志会被保存在图书馆里或者在线备份。这种方法可以提供较高程度的保证，证明你在报纸发出的当天就已经知道这个结果了。以后，当你想要披露你预测的结果时，你可以在同一个报纸上刊登第二份公告。

比特币里的安全时间戳

如果我们想用比特币而不是报纸来实现时间戳的功能，我们应该在哪里放置约定的哈希值？是在交易中的某个环节，还是直接在一个区块里？

人们想出来的第一个也是最简单的解决办法是，直接把钱打到数据的哈希函数值，而不是公共钥匙的函数值。由于你不知道对应地址的私钥，这样做会“消耗”这些币，让它们销毁掉，并且永不能被利用。为了降低成本，你可能需要发送微量的币值，比如1聪（satoshi，0.0000001个比特币，这是比特币的最小交易额）。

这个方法虽然很简单，但消耗比特币的做法不讨人喜欢（即使和交易费相比，这种被消耗的比特币量级可以忽略不计）。更大的问题是，因为比特币矿工不知道这些交易开支是永远不可用的，他们会永远地追踪下去。因此整个比特币社区对这个方法都不太感冒。

另一个较为先进的被称为**承诺币**(CommitCoin)的方法，是将你的数据编码进私钥里。第1章中曾经提到过：“使用ECDSA时，确保随机性良好来源至关重要，因为不良来源将可能导致密钥信息的泄露。这一点不难理解，如果你使用了不良随机源来生成密钥，那么该密钥就可能不安全。但是ECDSA的古怪就在于，即使你仅仅只是在生成签名时使用了不良随机源，而你使用的密钥完美无缺，你的个人密钥还是可能会被泄露。”

承诺币利用了这个特性。我们生成一个新的私钥把我们的数据约定进行编码，并对应地生成一个公钥。然后我们会发送一个微小金额的交易（比如2 000聪）到那个地址，随后再发送两笔每次1 000聪的交易回来。最重要的是，当发送回来的时候，我们会用同样的随机源来对两次交易进行签名。这样，任何人在区块链里计算包含被封装的数据约定的私钥时，必须使用两个签名。

比起把数据约定编码到公钥的方法，承诺币避免了消耗额外的比特币，而且矿工不再会一直追踪一个永久不能再被使用的支出。不过这个方法十分复杂。

不能被再次使用的输出

一直到2015年，比特币实行时间戳的办法是用一个OP_RETURN的交易，这个交易的输出可以被证明，但不能被二次使用（见图9.2）。这个OP_RETURN指令会立刻返回一个错误代码让这个脚本永远不能成

功地执行，这样一来，所封装的数据就被忽略了。就像我们在第3章看到的，这既可以用做消耗证明，也可以用来编码任意数据。到2015年，OP_RETURN允许输出80个字节的数据，这对哈希函数来说是足够了（SHA-256需要32个字节）。

OP_RETURN < H (data) >

图9.2 用OP_RETURN指令的时间戳

注：这是一个“不能被再次使用”的交易输出脚本，中间封装了一个数据约定。

这个方法“挤出了”在没有被使用过交易支出里的“水分”，因为矿工会精简OP_RETURN里的支出。这个数据约定的花费其实就是一个交易费。在整个2015年，一个典型的交易费通常小于1美分。这个交易费可以分摊在针对多个数据的一个约定上，从而使得成本更低。在2015年年末，已经有几个网站在做这些服务。它们收集不同用户的一组数据，把这些数据封装到一个梅克尔树中，然后发布一个包含了这个梅克尔树树根数据中不能被再次使用的交易支出。这种做法就好比，把当天需要实行时间戳的所有用户数据封装到了一个数据约定里。

非法内容

区块链随意封装数据的特性也有不好的地方，可能会被某些人恶意使用。在大多数国家，有些内容，尤其如儿童色情，它的制作和传播都是非法的，并且会伴随非常严厉的处罚。著作权法也严格规定了某些内容的传播。

当然，不少人已经尝试这样做去“危害”或者扰乱比特币社区。比如，有报道称有部分色情链接被公布在比特币的区块链上。这些害群之马的目的，就是让下载比特币区块链到个人硬盘并且运行完全有效节点的行为变得很危险，这也意味着你有可能存储和传播了这些非法的信

息。

然而，截至目前，还没有好的办法来阻止这种写入任意数据到比特币区块链的行为，即使我们用P2SH（支付给脚本的哈希值）来防止恶意攻击行为，也只不过是使交易多花些费用而已，无法完全阻止这种行为。

好在法律不是计算机算法，尝试用技术的手段对法律进行“黑客攻击”虽然很诱人，但并不容易。法律是需要人类来解释的，并融合了其他因素，比如我们的意图。以美国联邦法案2252号为例，其中在描述有关拥有、分发传播和接收儿童色情制品的非法行为时，使用的措辞就用了“明知故犯”这样包含了意图的关键词。

另外一个值得注意的是，根据上面我们讨论过的字节大小的限制，图片数据（除非是非常小的图片）不能直接被写在区块链的数据块中，这些数据要么被存放在只在区块链中保存相应链接的外部数据库中，要么是用一种冗长的办法封装在多个交易之中。最终的结果就是，大多数比特币用户都没有能力在交易中直接解码并查看数据，更不用说解码并查看跨越多个交易的数据了。

依附在比特币上的附着币

从好的一方面来说，因为我们可以把任何数据都写进比特币的区块，从而在比特币的系统之上建立起一个全新的货币系统，而不需要开发一个新的共识机制。我们只需要简单地把比特币用作一个只能被添加的记录，然后把我们的开发新币所需要的所有数据写进比特币的区块链。我们称这种方法为一个依附在比特币上的“**附着币**”（overlay currencies）。比特币成为一个底层基础架构，所有附着币的数据，通过以不可消费的交易支出的方式写进比特币的区块链。

当然，比特币的矿工不会验证你写进区块链的数据，因为他们不知道也并不关心这些数据在你所定义的新的货币体系里是否正当有效。只要你肯付交易费，任何人都可以写任何东西。不同的是，你必须自己开发更加复杂的逻辑来验证新货币体系里的交易，然后在每个收发这种新币的客户端（也就是钱包软件）都必须有这套逻辑。

举例来说，一个附着币的矿工不能再拒绝双重支付的交易。相反，每个附着币的用户必须检查区块链里的历史记录。如果有人尝试重复支付这个币（已经被用过一次了），那样第二次的交易就应该被直接忽略。因为这个缘故，在附着币里没有一个轻量级的SPV客户端。

合约币（Counterparty）是其中一种比较优秀的附着币，所有合约币的交易都被写入比特币的区块链，在2014年，大约有0.5%~1%的比特币交易携带了合约币的数据。同时它支持的功能也比比特币更多、更丰富，因为合约币不需要开发新的共识机制，而比特币的矿工也不需要了解合约币的规则，合约币的开发者可以集中精力开发一些有趣的功能，比如智能合约、用户自定义货币等。合约币的API也比比特币的API丰富很多，因为比特币的矿工不需要理解或者是批准这些API的开发。

不需要开发新的共识机制就可以创造一个新的数字货币，这种可能性是十分诱人的。你甚至不需要去鼓励新矿工们来加入你的系统，也不需要去改变比特币就可以增加新的功能特性。但是，这种系统还是依赖于比特币的，比如，这些附着币的交易费规则就受制于比特币。另外，由于附着币上的节点可能需要处理大量的数据，而比特币不会帮你去过滤这种交易，这种方法也有可能是低效率的。

9.2 比特币作为一个“智能资产”

我们现在来探讨一下，除了货币功能，比特币平台的其他特性。

我们在前面第6章中谈到，你可以简单地通过跟踪交易图谱，就可以在比特币系统里追踪一个币的所有权。请记住这一点：没有一个具体意义上的比特“币”，只有未消费的支出，我们把它们叫作币。每个比特币都有一个历史记录，任何人都可以在区块链里查询到。一个币的历史记录可以追溯到一个或多个原始交易，这些原始交易标志着这个比特币的诞生。正如我们之前讨论过的，在比特币里，匿名性其实是个伪命题，因为你可以通过这个方法去追踪比特币的所有权。



可互换性 (fungibility)

比特币的这个特征让我们发现了它的一个有趣的现象：比特币不是可互换的。在经济学中，一个具备可替代性的商品是指所有的个体是相同的，然后可以互相替换。比如黄金就是可以互换的，一盎司纯金可以和另一盎司纯金互换（因为它们之间没有任何差别）。但是比特币不一样，每个比特币都是独一无二的，因为每一个比特币都有着自己独特的历史记录。

在很多场景下，不同的历史记录可能不会有什么差异，但是如果特定的历史记录对某些人比较有意义，那么在你和他们交易的时候，你的一个比特币和他们的一个比特币就不一样。可能有些人不愿意用他的比特币来和你交换，可能因为他更喜欢他的比特币的历史记录，例如，部分重视旧币价值的收藏家们，可能觉得从创世区块里造出的币有着特殊的价值。

智能资产

比特币的这个可追溯性特性有什么作用吗？我们已经看到它可能会危害比特币的匿名性。接下来，我们要看一下为什么比特币的历史记录会有意义。

让我们先思考一下，怎样让一个普通的线下的物理货币有意义？假设我们想要在物理货币中加载一个元数据，事实上已经有人在这么做了。例如，在纸币上涂些文字，通常是一个笑话或者是一种“政治宣言”。但这么做纯粹为了好玩，并不影响纸币的价值。

但如果我们可以把证实过的元数据“黏”在我们的货币上，而这些元数据不是轻易就可以复制的，又会有什么结果呢？有一个做法就是把加密签名包含在元数据内，然后把这个元数据和钞票上的序列号进行绑定。

但这又有何用呢？比如一个棒球队，如果想用纸币作为门票，那么采用这个做法，他们就不需要花费大量精力去印制门票，也不用担心有人会去伪造门票。纽约扬基队可以宣称一张有特殊序列号的美钞可以作为一场特殊比赛的入场券，并且指定到某个特定的观赛席。这些特殊的纸币可以采用与其他门票同样的方式分发，比如邮寄给在线购买球票的球迷。任何拥有这张特殊纸币的人，都可以凭此进入体育馆，并坐在指定的座位上观看比赛。这张纸币本身就是门票。

扬基队可以用数字签名来增加真实性。他们可以把特定的比赛日期、座位号及钞票的序列号一起做签名，然后把这个签名印在纸币上。通过一个简单的二维码就可以实现这个功能（如图9.3所示）。球馆可以相应地维护一个保存所有钞票序列号对应每场比赛和座位号的数据

库，当你凭票入场的时候，它们只需要根据你所提供的二维码去数据库里校验即可，也就不需要在纸币上盖章并印上相关信息了。



图9.3 一张普通的钞票上设置一些有用的元数据

但这样做究竟有什么好处呢？现在，纸币可以代表许多事物。上述例子中，纸币替代了体育比赛门票，除此之外，纸币还可以有其他许多应用。为了纸币不能被伪造，政府投入巨大，我们可以利用纸币上已具备的防伪特性，来创建其他应用。当然，这张纸币的本身价值也保存了下来。当一个球迷使用了这张门票后，这张纸币还可以正常流通。当然，如果每个人都想在钞票上印一个元数据可能会有问题，但我们可以用数据库的方法来规避这个问题。

当然，这个新的元数据是否有意义，完全取决于我们对数据发行者的信任。在上面这个例子中，一定有人知道存在一个特定的“密钥”来签发有效的扬基队球票，或者下载整个扬基队的数据库以识别这个特殊纸币的门票价值，而对其他人来说，这就是一张普通的一美元纸币。无论如何，这是一个不错的属性，因为一旦在这张“门票”完成使命之后，它又可以作为普通纸币进入货币流通。

染色币

在比特币上，我们是否可以采用类似的数字化的方式增加元数据呢？我们想保留比特币好的特性，比如可以在线交易、快速结算，以及不依赖于银行。

顾名思义，**染色币**（Colored Coins）就是把比特币“染色”，即使这个币几经倒手，我们也可以根据这个特殊的“颜色”来追踪比特币，就如同在物理货币上印上一个代表特殊数据元的图章一样。一个“染色”的比特币依然可以作为一个有效的币，只是携带了额外的元数据。

为了做到这一点，在一个被称为“发行”的交易里，我们嵌入一些额外的元数据来宣布某些比特币具备了特定的颜色。如图9.4所示，在一个交易的支出中，我们发行了5个“浅灰色”的比特币，同一交易支出里的其他的7个，仍然是普通的没有染色的比特币。另外一个人，可能持有一把不同的签名密钥，在其他的交易里发行了“深灰色”的比特币。我们称之为“染色”，是为了便于直观理解。在实际中，所谓的“颜色”其实就是一串二进制的数字代码。这里，最重要的一点特性是，同样颜色和同样价值的币是完全相同的。

虽然我们现在有不同颜色的比特币，但依然可以进行正常的比特币交易。我们可能碰到一个交易，它包含了几个不同输入的比特币：有些是深灰色的，有些是浅灰色的，有些是没有染色的，并且混在一起。同时，这个交易可能会有几个支出交易，其中的比特币保持着被染色的状态，并且交易中可以添加一些元数据，决定这些比特币根据染色的不同去往不同的交易支出，我们可以把一个包含4个深灰色币的支出拆分成两个更小的深灰色币组合，我们也可以把几个深灰色币组合到一个大的深灰色币交易中。

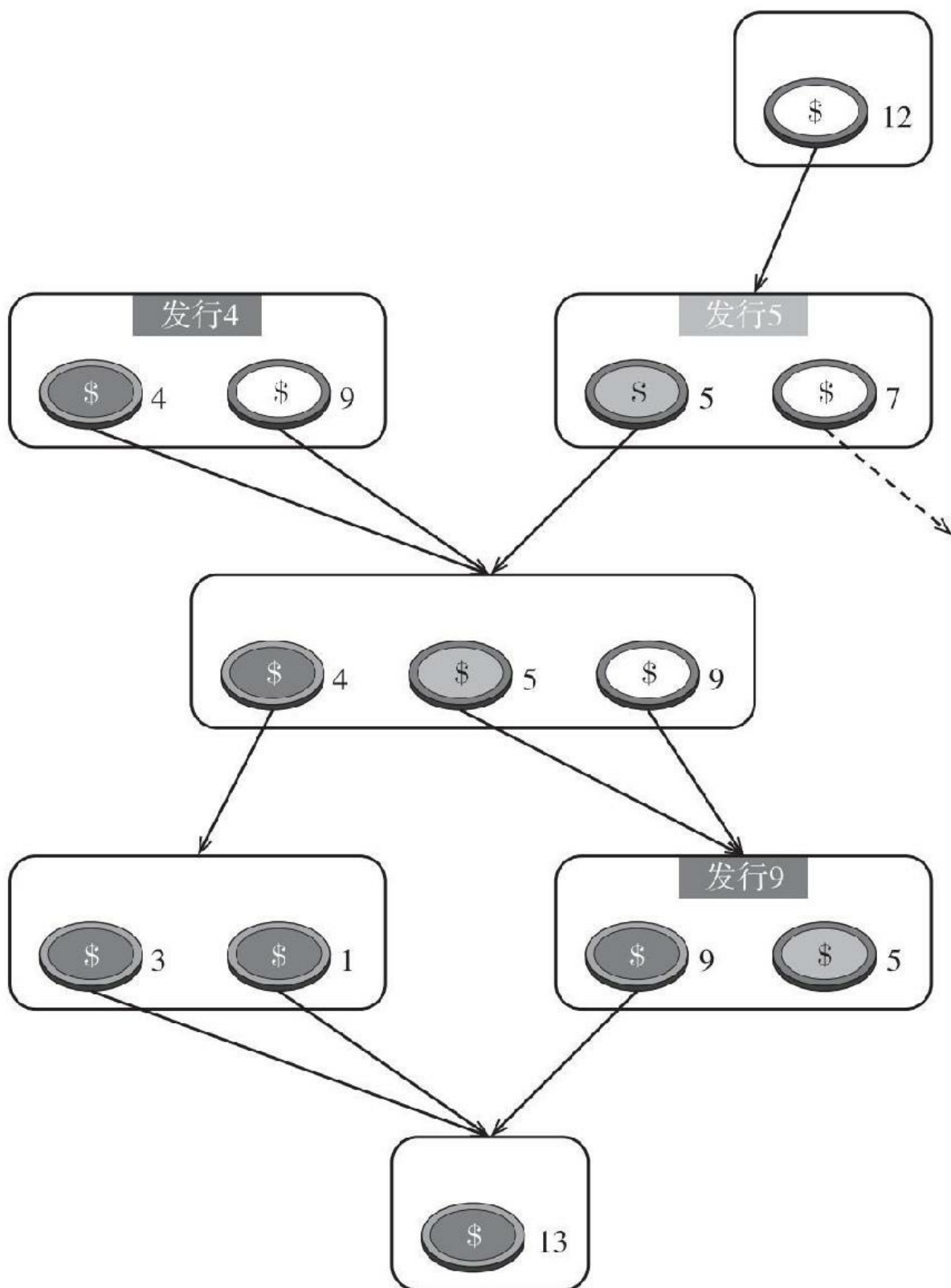


图9.4 染色币

注：交易图谱描述了染色币的发行和传播过程。

开放资产

2015年，在比特币里实施“染色”的、最受欢迎的应用方案是“**开放资产**”（OpenAsset）。资产通过一个特殊的支付给脚本的哈希值（P2SH）的地址来发行。如果你想发行染色币，首先要选择一个P2SH地址。任何通过这个地址转账的币在进入的时候都没有颜色，在出来的时候，就会被这个地址分配一个特定的颜色。如果让这个染色币变得有意义，你还要把这个地址公布出来。有许多交易所会追踪这些地址来推断比特币染上何种颜色。由于比特币可以按照时间顺序通过多个地址进行染色，因此，一个比特币被染上多个不同的颜色，也就不足为奇了。

一旦执行了一个带有染色币的交易，你就必须嵌入一个有特殊标记的支出，就像我们给数据约定加时间戳一样，这是一个可证实且不可再次消费的支出。被封装在这个有特殊标记的支出里的元数据，详细地列出了染色的输入是如何分配到不同输出的。

正如我们之前所注意到的，比特币对此完全兼容，因为它并不对比特币做任何改变，矿工社区也没有对这种做法多加干涉。无须中央权威授权，它允许任何人对货币进行各种染色。只要有人理解、认可并遵循你所设计的染色币的规则，那么你所发行的染色币甚至有可能超过比特币本身的价值。比如，如果扬基队发行染色币，并且这些币可以作为球场入场门票，只要球场的管理员认可这些染色币的门票特性，他们就会让你凭票（染色币）入场。

这个方法的第一个缺点是，我们必须把不可被再次消费的标记支出放进每个交易里。由于每次交易一个染色币时，都需要多花一些交易费，这会增加一点成本。第二个缺点是，矿工只会验证作为底层基础的

比特币的有效性，但不会去验证染色币的有效性。如果想要验证一个染色币的有效性，你必须亲自去查证它所有的历史记录，或是委托第三方来帮你完成。此外，不同于一般的比特币，用户不能使用一个轻量级的简单支付验证客户端。这就使得类似手机这种有计算性能限制的设备，在使用染色币时变得非常困难。

染色币的用途和智能资产

一个经常被引用的智能资产用途就是公司股票。一个想要用染色币来发行股票的公司，需要公布一个发行地址和规则，通过这个地址发行的染色比特币代表了公司的股票。1聪比特币就可能代表公司的1股。股票持有者就可以在区块链上交易股票，而不需要一个像股票交易所这样的中央媒介。当然，股票持有者必须信任公司对这种股权的认可。例如，公司承诺按照每股支付相应的股息或者授权股东对公司决策有比例性的投票权利。传统股票是通过法律规定来保障的，截至2015年，染色币或者其他基于区块链的资产还没有获得任何一个司法机构的认可。[\[1\]](#)

物理特性。 另一个可能的用途是，染色币可以代表现实世界中的一些资产。比如，一个染色币可以代表一处房产或者一辆汽车。你所拥有的一辆高级轿车可以和一个在区块链上的特定的染色币关联，然后持有这个染色币的人可以用它来启动和驾驶这辆车。当你要卖这辆车的时候，或是至少要转让使用权的时候，你只要在区块链里简单地执行一个单笔交易。在第11章，我们将探讨在技术上如何实现这个功能，以及一些可能会遇到的社会和法律上的障碍。但是，由于其具备了智能特性，我们的梦想是让现实世界中任何有形资产都可以用染色币来代表，并且资产的转让或交易就像比特币的转让或交易一样容易。

域名。 最后一个例子是，使用染色币来完成一些现有域名系统的

功能：登记和转让拥有权，关联域名和IP地址。域名市场有许多有意思的特征，其中之一是它有无数可能的域名。根据域名名字是否方便记忆以及其他因素，域名有着不同的价值；同样，对于不同的人，一个域名可能有完全不同的意义。我们可以用染色币来处理域名登记和其他相关功能。事实上，有一个另类币就是为这个目的而设计的，叫作域名币（Namecoin），我们会在第10章中做具体讨论。每个方法都有自己的独特优势，染色币可以获得比特币区块链的安全保护；而另类币可以相对容易地部署域名登记、转让、关联IP等复杂逻辑。

[\[1\]](#) 2016年3月，美国在线零售商Overstock已经获得了美国证券交易委员会（SEC）的批准，通过比特币区块链技术发行100万股新股。——译者注

9.3 多方参与的安全博彩系统

我们现在来讨论一下如何在比特币里举行一个“掷硬币”的游戏。首先看一下，在线下是如何建立这个系统的。

爱丽丝和鲍勃想要下一个5美元的赌注。他们在下注之前商量好了游戏规则。鲍勃往空中扔一个硬币，爱丽丝在硬币落地之前叫出“正”或“反”面。当硬币落地的时候，可以立即判断谁是赢家。双方都知道这个结果有足够的随机性，他们之中任何一人都没有办法影响结果。

为了使双方相信这个游戏是公平的，游戏的步骤顺序以及硬币的特性至关重要。但上述设计有一个缺陷，就是他们二人都必须同时在场，而且相信对方会愿赌服输。在线上，我们也想设计一个同样“公平”的博彩系统，同时确保输家也会愿赌服输。

初看起来，这个应用有些古怪，并且有局限性，并不值得深入研究。非常有意思的是，一个基于比特币的在线博彩系统中本聪之骰，已经被证明非常受欢迎，但它并未采用上述设计模式，而是依赖于某一方的信用，但它时不时地囊括了大部分比特币网络上的交易量。

我们想研究这种加密数字货币的“掷硬币”系统的真正原因是，如果我们可以据此设计一个安全协议的话，也可以用这个技术来设计其他有趣和有用的协议。密码学专家研究“多方参与的安全计算”，也就是说多个互相不信任的参与者，每个主体都有各自的数据，然后综合各主体的数据来共同计算一个结果，但同时每个主体都不想让他参与者知道自己的数据是什么。想象一个类似的场景，一次竞价拍卖，但没有一个可靠的拍卖行。通常这些计算需要被随机化，来打破互相之间的关联，最后，这个计算的结果是有金融属性的，并且是不可逆转的。比如，我们

想要保证中标者最后会付款给拍卖物品的卖方，更进一步，让卖方的（智能）资产自动转移到中标者的名下，甚至更进一步，我们还想要惩罚那些不守规矩的人。

总而言之，一个安全的多方博彩系统虽然看起来简单，但其实可以用来研究一个非常强大的系统模式：各自都有敏感数据的互不信任的一群参与者，共同来执行一个程序，不仅仅是为了控制数据，还可以控制与之关联的资金。

在线掷硬币系统

第一个挑战是找到与“掷硬币”相对应的一线上的相关方法。假设我们三个参与者：爱丽丝、鲍勃和卡罗尔，大家都想以相同的概率来选择号码1、2、3。我们尝试以下协议：每个人选择一个大的随机数，比如爱丽丝选 x 、鲍勃选 y 、卡罗尔选 z ，然后互相告知各自的随机数，并共同计算结果 $(x+y+z)\%3$ 。

如果他们完全是完全独立地选择随机数的话，这个方法是可行的。但请记住，这是在互联网上，没有办法可以限制他们绝对地“同时”送出数据。爱丽丝可能会等到鲍勃和卡罗尔送出随机数之后再发布她的数据。这样一来，她可以轻易地操纵这个计算的结果。我们没有办法设计出一个数据交换协议，它可以让大家相信没有人会作弊。

为了解决这个问题，我们还是要回到函数约定。首先，每一个人选一个大的随机数，并发布它的哈希函数值；然后，每个人披露各自所选的数字；接着，其他两个人查证这个被披露的函数值和在第一步发表的数据是否正确；最后，计算这个三个随机数的结果，如下：

第一回合：

每个参与者选择一个大的任意字符串。爱丽丝选 x ，鲍勃选 y ，卡罗尔选 z 。

每个参与者发布对应的哈希函数值 $H(x)$ 、 $H(y)$ 、 $H(z)$ 。

每个参与者验证 $H(x)$ 、 $H(y)$ 、 $H(z)$ 具有明显的差异性（否则放弃这个协议）。

第二回合：

三个参与者分别披露他们所选的字符串 x 、 y 和 z 。

每个参与者查证这些字符串是否与第一回合里发布的函数值相吻合。

最后的输出是 $(x+y+z) \% 3$ 。

这种数据协议之所以能成功是因为以下因素：第一，因为函数的输入 x ， y ， z 是大的任意数，没有人可以在第一回合之后预测其他人的输入；第二，如果爱丽丝按照规则任意地选择她的输入，她可以相信，不管鲍勃和卡罗尔是否选择了随机数，最后的输出结果也是随机的。

公平性

要是有人不披露约定怎么办？在这个协议的第二回合里，假设卡罗尔一直等到爱丽丝和鲍勃披露他们的秘密随机数，然后，在披露之前，意识到她会输掉这一局，她就有可能拒绝公布她的随机数——她可以说她忘记了或是假装下线。爱丽丝和鲍勃可能会怀疑，但他们也没有什么好的办法去追查。

我们所要做的是立下一个规矩：参与者若是做出承诺，则必须在一定的时间内披露所选的随机数。在密码学里，这个特性叫作公平性。比特币提供了一个非常好的解决方法。

比如爱丽丝想要做出一个有时限的约定承诺，但鲍勃是唯一对此有顾虑的。第一，爱丽丝先设置一定的保证金，比特币支出交易的脚本可以用来规定，这笔保证金只能用以下两种支付情形：第一种支付情形是必须同时有爱丽丝和鲍勃两人的共同签名；第二种支付情形是只要爱丽丝披露了她的随机数，以后消费这笔交易，就只需要有爱丽丝的签名。如果爱丽丝所选择的随机字符串是 x ，那么输出脚本（ScriptPubkey）会包括哈希函数 $H(x)$ 的值。

接下来，爱丽丝和鲍勃会同时签下一个交易，把这个保证金支付给鲍勃（两种情形之一）。但为什么爱丽丝会同意这样做呢？这个交易带有一个`nLockTime`值来保障鲍勃不能在时间点 t 之前来赎回保证金。因为，在此时间之前，爱丽丝只要愿意披露她的约定随机值，她就可以赎回这个保证金，所以她的这个签名交易是安全的。见图9.5。

```
scriptPubKey:
  OP_IF
    <AlicePubKey> OP_CHECKSIGVERIFY <BobPubKey> OP_CHECKSIG
  OP_ELSE
    <AlicePubKey> OP_CHECKSIGVERIFY OP_HASH <H(x)> OP_EQUAL
  OP_ENDIF

scriptSig for Case 1:
  <BobSignature> <AliceSignature> 0
scriptSig for Case 2:
  x <AliceSignature> 1
```

图9.5 在有时限的哈希函数约定中使用输出脚本和输入脚本的交易输出

如果爱丽丝在弃局之前没有披露她的约定随机数值，那么鲍勃就可以在时间点 t 之后赎回该保证金。没有人逼迫爱丽丝披露她的随机数，但如果她不披露，她会因此失去预设的保证金。

我们如何用这个有时限的函数约定来实现安全的博彩系统？其实，架构和之前几乎一样，差别在于，我们不再采用简单的函数约定，而是采用有时限的函数约定。任何一方，要赎回这笔保证金就必须把正确的

随机数值 x 披露出来；如果在最后期限到来时还不披露出他的随机数值，就会放弃他的保证金，以用来补偿其他两个玩家。

可以在比特币系统上实施这个博彩系统。但这个系统有些复杂，而且有时限的函数约定还要求多个非标准的交易。当系统里有 n 个玩家的时候，由于每个玩家都要设置一笔保证金，我们需要 n^2 个约定，此外玩家们还不得不投入比全部赌注更多的资金用来托管保证金。但对于参与者较少的游戏来说，这是合理的，并且有更好的效率。最重要的是，这个游戏验证了本来认为不可能的数据交换协议，比如在线掷虚拟硬币，并对不遵守规则的玩家进行惩罚，在比特币的世界里是可以做到的。

9.4 比特币作为一个公共的随机源

在上一节，我们展示了一群人如何选择一个公平的随机数。在这一节里，我们将讨论如何用比特币来产生一个对任何人都公平的公共随机数。为什么我们需要一个公共随机数？让我们先看一下几个现实中已经存在的依赖公共随机数的案例。

NBA新人选秀

其中一个例子就是每年春天的美国NBA联赛的新人选秀大乐透。NBA联盟中所有的30支球队聚集在一起，根据上赛季每个球队的赛季排名增加相应的权重，随机选择球队选秀顺序。在1985年，联盟首次采取这种方法进行选秀，乐透选秀的过程通过电视现场直播，包含球队名字的信封在一个透明的转盘里被充分打乱，委员会专员随后去挑选这些信封。因为纽约尼克斯(Knicks)队获得了当年的状元秀中锋帕特里克·尤因(Patrick Ewing)，最终尤因也确实成为NBA名人堂的一员，当时这个乐透的产生引起了不小的争议。由于那次的乐透发生在纽约，其他球队的球迷宣称整个过程被人操纵，并偏向尼克斯队。

有很多有关NBA是如何操纵选秀过程的阴谋论，比如著名的“折角”论(“bent corner” theory)是说包含有尼克斯的信封有一个角被故意折弯了，这样委员会专员通过触摸就可以分辨出哪个信封是尼克斯的。另外一个论调是说尼克斯的信封之前被放在了冷冻室里，这样专员可以通过选择一个手感比较冷的信封来挑选出尼克斯队。这些论调都反映了一个事实，这种类型的选择要做到绝对公平是非常困难的，有很多合乎推理的作弊空间，想象一下一个职业魔术师的巧手可以做些什么！直到今天，选秀乐透每年都会举行，但每一次都充斥着各种阴谋论和谣言，

以说明选秀并不是绝对公平的。

美国军队选秀

另一个更加严肃的案例是1969年的美国征兵选秀，用于决定哪些年轻人会去参军，大部分被选中的人事后都被派去参加了越南战争。同样使用了一个类似于NBA选秀的方法，由美国国会派出的代表来主持选秀并通过电视直播（如图9.6）。他们在一个大的塑料桶中放了很多小球，每个小球包含了一个数字，然后轮流从桶中把这些数字小球取出来，根据数字所代表的生日来决定优先级，根据这个优先级挑选合格的年轻人参军。



图9.6 1969年（越战）军队选秀

1969年的这次征兵选秀，是首次在全国范围内采用乐透方式进行选秀。其目的是通过避开数以千计的本地征兵委员会，以使选拔过程更加公平，并且向公众公开这个过程。但遗憾的是，这个选秀乐透也演砸了，不到一个星期，概率专家通过数据调查分析注意到了一个特别的模式（如图9.7所示）：出生于下半年的人被选中的优先级较低。虽然这

种差异非常细微，但是从概率统计上是非常显著的，说明这不太可能是偶然事件。当他们回看现场录像的时候，发现每次转动转盘的次数恰恰都是偶数次，这意味着一开始是上层的小球有较大的概率一直留在上层，说明为了形成随机抽签的混合程序并不充分。

这两个案例都证明了，设计一个公众认可的随机过程并由此产生一个认可的公共随机数，是十分困难的。无论你采用什么方法，总有人怀疑你作弊。风险在于：这个随机过程可能会被操作——即便这个过程是真正随机的，但公众并不信任它。[\[1\]](#)

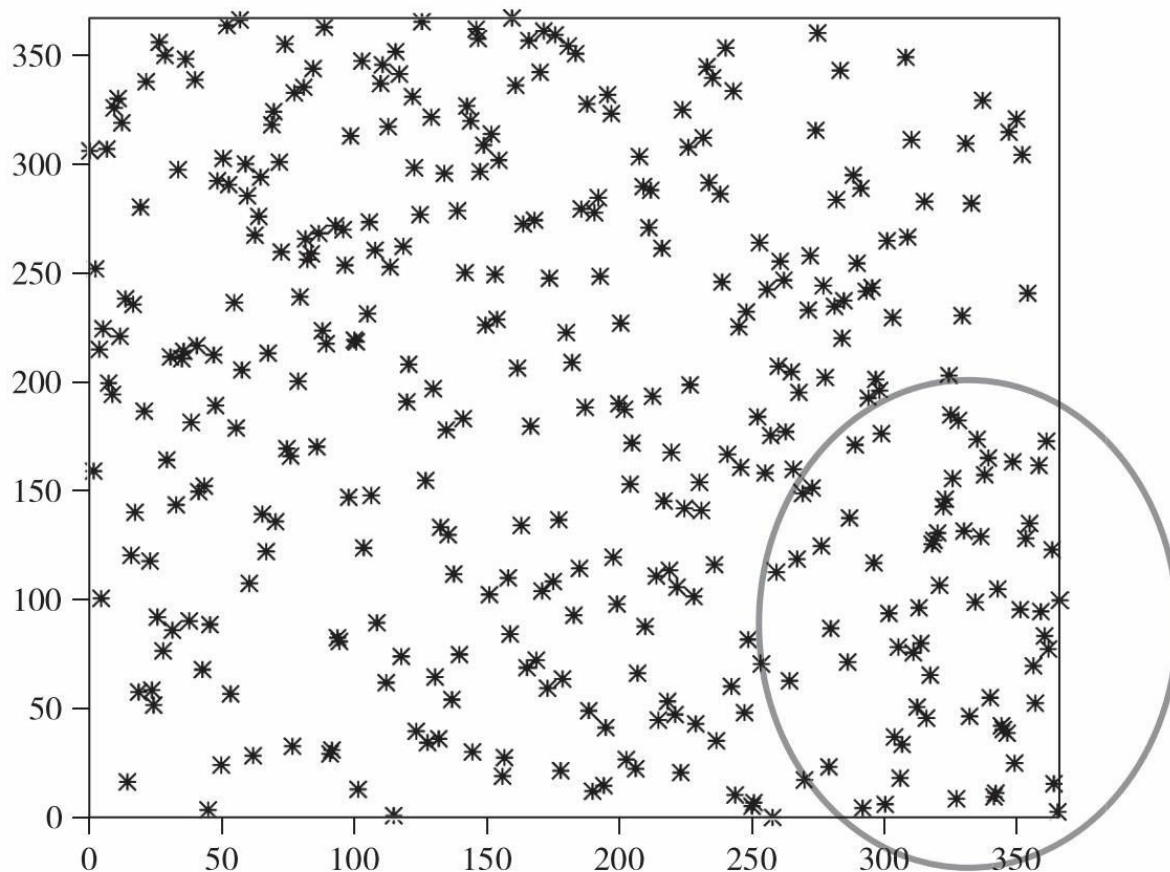


图9.7 1969年征兵选秀的概率统计偏差

注：x轴代表日期，y轴代表选秀号码。

密码学“信号塔”

由于成本低，并且大众易于理解，用转盘、抛硬币、掷骰子等方法去展示公开随机性，在历史上一直比较普遍。但是这些方法非常难以审计，因此并不适用于大范围的场景。即使整个过程从视频上看起来是合法的，人们也有理由去怀疑乐透的执行者可以使用“魔术师之手”去操纵结果。

那么，通过密码学的办法，我们是否可以做得更好？这里，我们用密码学“信号塔”（cryptographic beacons）来特指一个提供公共随机源的

服务。我们的想法是“信号塔”会源源不断地在一个固定的频率产生随机数，并且没有人可以预测这些随机数。只要大家同意这一点——没人可以预测这个信号塔的下一个输出，那么大家就都可以相信其生成的是一个真正的随机数。

一个完美的密码学信号塔可以服务于各种公开乐透项目，比如上面两个例子。如果你想要在本地的俱乐部玩一个宾果（Bingo）游戏^[2]，你再也不需要用一个大的转盘来产生随机性了。只要每个人都信任信号塔，就不要用物理的方法来展示随机性了，这会省去很多麻烦。

密码学专家提出了很多其他的公共随机源的应用方案，包括投票系统、零知识验证、分割选择协议等。如果你有一个完美的密码学信号塔，其中很多方案都会变得非常简单有效。但遗憾的是，截至目前，我们还没有找到一个完美的方案去打造这样一个信号塔。

NIST信号塔

NIST，即美国国家标准与技术研究所（National Institute of Standard and Technology）。从2011年开始，NIST运行了一个它们自己的信号塔服务。它们声称用了一个非常复杂的实验室装置来产生随机数，甚至动用了两个纠缠态光子。由于随机数是由量子力学现象产生的，那么理论上这个数字可以保证非常强的随机性。如果你认可海森堡不确定性原理（Heisenberg uncertainty principle）和其他一些被广泛接受的物理学原理，那么你就会相信这个信号塔产生的数是真正随机的，并且不可预测。NIST信号塔服务可以每60秒产生一个附带有数据签名的随机数，并提供一个非常便利的程序接口——服务可以通过网页来访问并返回随机数。

从某种意义上说，NIST信号塔代表了从物理上展示随机性的极

限，但无法解决一个基本的信任问题——你必须信任NIST确实是通过它们所宣称的这些程序来产生随机数的，你必须信任在马里兰州的某一个建筑里面，NIST确实用它们的实验室来产生这些随机数，而不是伪造的，你还必须信任它们确实没有能力故意重写其中一些随机数。

打造一个信号塔的其他潜在方法：自然现象

我们是否可以使用一些每个人都可以观测到的自然现象来实现信号塔？或者我们可以使用天气的一些细节，比如在某天某个特定地点的温度，或者是风力的强度，或者是否会下雨。当然，我们有能力去提前预测天气，但是预测的结果并不是非常精确，所以我们可以使用这些测量值的“最低有效位”。但是这个方法也有局限性，那就是需要所有的参与者在同一个地点做同样的测量。

为了避免这个问题，我们可以利用太阳黑子，一种太阳表面的爆发活动（见图9.8）。另外一个例子是宇宙背景辐射，通过广播天线，你可以从地球上的任意一点都可以监测到这个数据，而且每个人都可以读取到同样的数值。这些都是超大范围发生的现象，很容易向公众证明没有其他人可以操纵这个过程。想象一下，某人穿越宇宙到达太阳表面，然后用某种办法去影响太阳黑子现象，而其目的仅仅是为了操纵地球上的某个乐透项目，这显然是不现实的。所以上述这些方法都有很好的特性：公众可观测性、可防止被操纵性，以及一个可接受的不可预测性。

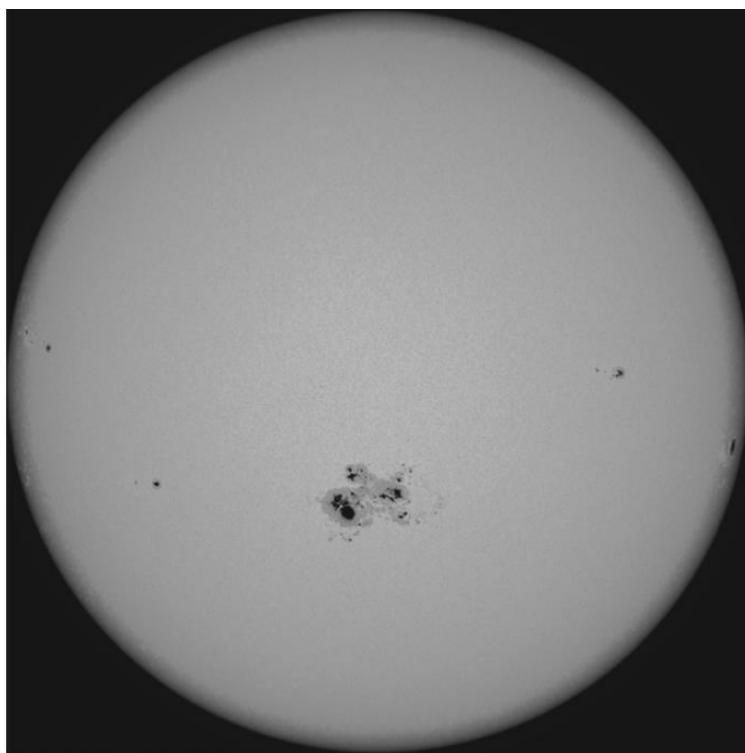


图9.8 NASA太阳黑子照片

但上述这些方法都有一个共同的问题，就是生成随机数太慢了。例如，如果随机信号是当日最高温度，那么你每天只能获取一次这样的数值；太阳表面也不是经常变化，在很多密码学应用中，随机数通常作为伪随机数发生器（Pseudo-Random Generator，简称PRG）的输入，从安全角度考虑，这些输入通常需要达到80比特位长度，甚至更多，但如果以天气或者天文学为数据源，那我们可能需要很长时间才能积累到80位长度的随机数。

另外，观测太阳黑子现象这种方法还需要专业技能，所以你还需要依赖一些可信任的专业观测者来获取这些测量数据。由于有很多这样的可信任的观测者，我们也希望他们“互相之间有诚信”。信号塔的应用者，或者说是这些应用的用户，可以随时选择并替换观测者。这个特性被称为“信任的敏捷性”，相比于NIST是提供信号塔服务的单一机构，这个特性更加优越。

还有更深层次的问题，虽然这个问题看起来可能微不足道，那就是，我们是否可以找到一个方法，它可以使一个现实世界的观测数据——例如温度、太阳黑子图——转变为一个数据字符串，并且它还需要保证每一个观测者都获得相同的字符串？我们可以尝试数字化这个观测数据：比如，我们用华氏度来描述温度，并使用第一个十进制数位作为信号塔的输出，但是除非每一个观测者的温度计都是不可思议的精准，否则就会出现下面的情形，有些观测者读取的温度（比如）是62.7，而另外一些人读取的则是62.8。目前看来，不管我们选择哪种自然现象或者采用哪种协议，我们都会遇到这种“极端情况”。对于一个密码学信号塔，即使测量值出现非连续性的可能性非常小，那也是无法接受的，因为这有可能使得PRG产生的随机数变得完全不同。

金融数据

还有一个类似的想法是使用金融数据作为数据源，比如股票市场价格指数。同样，这些是公开的可观测的数值，而不像自然现象，这些金融数据本身就是用数字来呈现的，所以不会因为观测者不同，产生数据不一致的问题；同时，我们有很好的理由相信，股票价格的小波动是很难预测的：如果你可以预测纽约证交所某一只股票的交易价格，并且精确到美分级别，你就会成为一个非常赚钱的日内交易员。某些人可以通过买卖股票，去操纵股票价格到某一个特定的数值，但这需要巨大的成本。

但是，这种方法也需要依赖某一个信任方，比如股票交易所。即使股票交易所本身有很强的意愿去建立自己的诚信，但如果让它们操纵一个非常有利可图的乐透，那么它们就有可能去尝试改变股票价格（例如，通过插入自己的买卖单）。

截至目前讨论的方法，似乎很难去规避信任方的问题，而这个信任

方却是可以在整个过程中的某些关键环节对结果施加重要影响的。

用比特币作为一个“信号塔”

幸运的是，把中央权威从数据交换协议中剥离出来，在之前认为几乎是不可能的任务，而比特币是很有希望实现这一任务的技术，而这也是本书的中心思想之一。我们是否可以把比特币作为一个生成随机数的“信号塔”呢？我们想要从比特币的区块链里摘取随机数，与此同时保留比特币所有去中心化的特点，正是这些特点使比特币如此吸引人。

我们回忆一下，矿工必须计算大量的随机哈希函数来找到一个有效区块。或许这意味着没有人可以不经过挖矿工作就能预测或是影响下一个区块的生成。当然，任何一个区块的哈希函数结果的最初几个字节都是零，但是在合适的假设下，唯一可以预测剩余位数的比特值的方法可能是找到一个胜出有效区块，然后选择性丢弃它（见图9.9）。

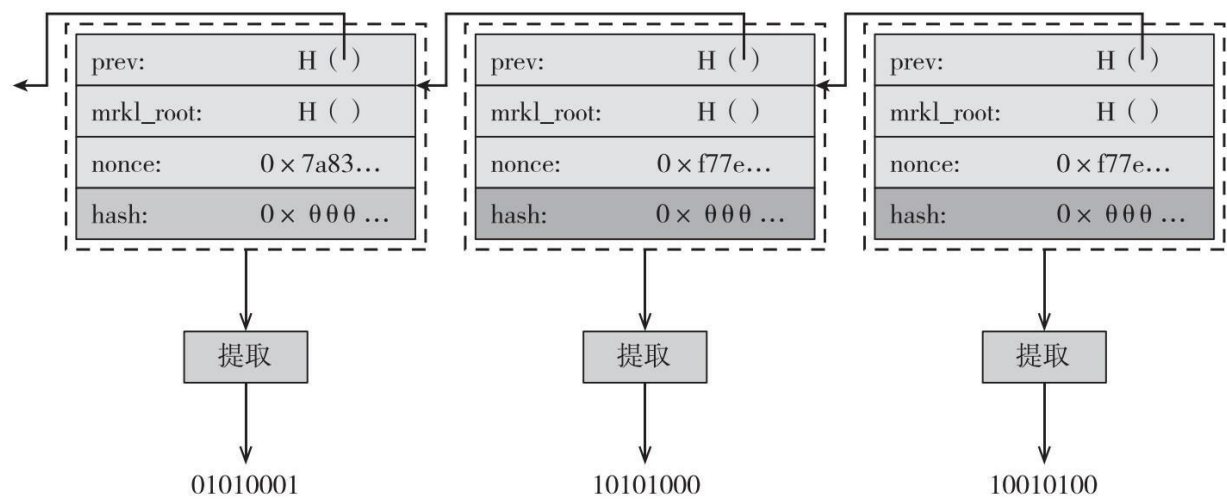


图9.9 比特币像灯塔一般

注：我们可以通过使用随机提取功能，提取公共随机数据，标注区块链上的各个区块。

这样一来，把区块链变成一个随机数“信号塔”成了一件简单的事。

在区块链上的每一个区块上，我们在区块头部设置一个“随机数抽取器”。随机数抽取器，其实就是一个哈希函数，这个哈希函数把所有的输入随机熵均匀地压缩成一个随机字符串。每次只要发表一个区块，我们就有了一个新的随机信号输出。

评估比特币“信号塔”的安全性

假设你参加一个乐透抽奖，这个抽奖的结果是由未来将要产生的、一个预先设定的、位于高度 h 的某个区块的输出所决定的。这个乐透抽奖有 N 个参与者，每个参与者都下注了 B 个比特币，如果你也是一名矿工，我们再假设，你幸运地找到了一个区块 h 的函数解谜的答案，你就可以选择发表或是不发表这一区块。如果你不喜欢从这个区块里产生的抽奖的结果，你可以轻易地丢弃这一区块，然后让其他找到这个区块的人来决定这个抽奖结果，但同时，你必须放弃因为找到这个区块所带来的收入。

让我们计算一下，下注的数额 B 值需要多大，才值得考虑放弃区块本身的奖励。如果你成功地找到了一个位于高度 h 的区块来决定抽奖的结果，然后意识到，如果你发表了这个结果，你肯定会输掉抽奖；如果你扔掉这块，你还是有 $1/N$ 的概率来赢得 $B \times N$ 比特币，这就意味着，如果你期望的抽奖奖励 $(1/N) \times B \times N$ 比特币比挖矿所获得的25个比特币奖励要大的话，那么放弃区块奖励是合理的（在2015年，如果不考虑交易费的话，区块奖励大概是25个比特币），所以如果 B 大于25，这种丢弃策略就是有利可图的。在2015年中旬，25个比特币价值大约在5 000美元左右。所以如果每个玩家下注不到5 000美元的话，并且假设每个玩家都是理智的，那么这个乐透抽奖是可以抵抗放弃有效区块这种攻击的。

另一大优点是这是一个完全去中心化的信号源，没有一个中心化的信托方。比起其他几个信号源的方案，它的处理速度相当快，大概每10

分钟就产生一个输出。然后通过上述的简单模型，我们可以估计一个攻击者想要操纵信号源输出所需要付出的代价。

用比特币作为信号塔办法的一个缺点是，不能精确定时。比如，假设我们想要在明天正午读取这个信号源的值，但我们无法知道哪个区块在哪个时点会生成最新的一个区块。虽然平均来说，在正午之前或之后的10分钟内一定会有一个区块被公布，但这还是会有误差。如果我们想降低目标区块在一个短分叉事件中丢失的可能性，我们还要对有可能发生的延迟有所准备。在比特币世界里，通常情况下要等6个区块（60分钟）后，才能确信这个信号值是真正地确认了。

另一个缺陷是，相对来说，操纵这个信号值所需的代价可能还是太低。如果我们用这个方法实行NBA选秀，由于其中可能涉及几千万美元利益，球队顿时就有了贿赂矿工来操纵选秀过程的动力。所以，当涉及巨额资金时，这个方法是否有效仍值得探讨。

最后，我们的安全评估忽略了一些现实生活中的因素。比如，对于加入某一个矿池的矿工来说，丢弃一个有效区块并不会让他损失很多钱，因为他们是根据贡献算力的比例，而不是区块来领取奖励的。所以，比特币信号塔目前还是一个有趣但没有被证明的想法。

脚本语言对信号塔的支持

如果我们扩展比特币的脚本语言功能，加入一个特殊的**操作码**（opcode）来读取比特币信号呢？按照最初的设计，现在的比特币脚本语言没有任何办法去实现任何随机性，因为矿工必须验证脚本，而且一个脚本的有效性需要获得所有矿工的认可，但如果我们用了信号塔产生的随机数，由于这是一个可被证明的公共随机数，把这个随机数加入交易脚本中，矿工就容易随机性地达成共识。

假设我们有一个操作码可以做一个随机的决定，这个决定是基于上一个区块的信号塔输出的。我们可以把整个复杂的抽奖数据协议用一个脚本来替代——读信号塔的随机数值，然后把该输出分派到n个密钥中的一个。这需要有多回合的数据协议安全保证或是有时效的函数约定。

这个想法的一个缺点是，为矿工操纵抽奖提供了可能性，如果他们发觉挖到的这一个区块里的交易会让他们输掉这个抽奖，他们就会简单地将抽奖交易延迟至后面的一块出现。但是我们可以对信号塔的操作码做一个小小的调整来防御这类攻击，也就是说，你不是用上一个区块，而是使用某一个特定高度的区块所产生的信号塔随机数。

[1] 所以一个公平的不受操纵的公共随机源是一个公共福祉，而比特币可以做到这一点，因为它是去中心化的。——译者注

[2] Bingo是一种填写格子的游戏，在游戏中第一个成功者以喊“Bingo”表示取胜而得名。——译者注

9.5 预测市场和真实世界的数据源

作为本章的最后一个论题，我们现在来看一下如何利用加密数字货币，以去中心化的方式来实现一个预测市场，与此相关，如何把真实世界的的数据导入比特币系统。

在预测市场中，人们可以在一起对未来的事件进行下注，比如体育比赛或是选举。对于事件发生的每一个结果，参与者可以买卖和交易相应的“份额”。

表9.1 2014年世界杯期间球队选择的预测表（数字代表在每个阶段下注某支球队捧杯所需花费的美元）

球队	德国	阿根廷	巴西	美国	英格兰	荷兰
赛事之前	0.12	0.09	0.22	0.01	0.05	0.03
小组赛	0.18	0.15	0.31	0.06	0.00	0.05
半决赛前	0.26	0.21	0.45	0.00	0.00	0.08
决赛前	0.64	0.36	0.00	0.00	0.00	0.00
决赛后	1	0	0	0	0	0

注：押注美国队赢得世界杯的价格在美国队小组表现出色后，从1美分上升到6美分。当巴西打进半决赛后，其赌注价格上升到了45美分，而当巴西队输掉半决赛后，这份赌注变得毫无价值。最后只有德国队的赌注才有价值，因为他们赢得了冠军。

我们用一个案例来详细解释一下预测市场背后的概念，使其更加清晰。2014年的世界杯在巴西举行，假设有一个市场，你可以买卖每个队的赌注。最终冠军队的赌注是1元，而其他队的都是0。比赛开始之后，根据市场认为每个队最后能赢得冠军的概率，每个球队的赌注都会有一个价格。表9.1就是五个队的赌注价格情况。

在比赛前，德国队赌注的交易价格是12美分，意味着市场觉得德国

队大约有12%的机会获得最后的冠军。当比赛进行的时候，这些赌注价格会上下波动，反映了市场参与者对每个队最终获胜的信心。

在我们的案例中，英国队赌注本来的交易价是5美分，但后来变成了0，因为英国队没有小组出线，他们已经不可能取得最终的胜利，价格也相应地反映了这一点。与之相反的是，美国队最初被认为很难从小组出现，但是结果他们的小组赛表现却相当不错，如果你在最初美国队赌注价格非常便宜的时候（1美分）买了它，并在它出线并变成6美分的时候马上卖出，你就可以拿回6倍于你最初的投资，而不需要等到全部比赛完了之后再卖出。虽然美国队最后没有赢得世界杯，但你还是可以在美国队小组赛表现抢眼的时候，通过市场对美国队的信心调整来获利。

半决赛的时候只剩下四支队伍了，由于美国队与英国队都被淘汰出局，所以他们的价格都是零。每个剩下的队都有一个高价位，他们的价格之和是1美元。巴西队价格最高，因为那时市场认为巴西最有希望赢。当巴西队输了半决赛的时候，它的价格马上变成了零。在两个小时内，市场对其信心就发生了戏剧性的改变。你可以对巴西队进行一个卖空或者去买其他球队。

到了决赛的时候，只剩下两个队。它们的价格总和还是1美元。当然到最后，德国队获得了最终的胜利，也只有德国队的赌注最终有价值（1美元）。

当然还有一个获利的办法就是，你在最初就以12美分的价格买下德国队的赌注，然后一直持有到最后，直到德国队获胜。这基本上传统体育博彩的机制——你在比赛前下注，然后在比赛胜利后收钱。但在一个预测市场里，有很多其他办法可以进行博彩和盈利。你可以在任何时间对任何球队下注，你是否可以获利完全取决于你准确地预测市场信心的转变，而与最后结果无关。

这里有另外一个案例，这次是一个完全真实的预测市场案例。在2008年美国大选之前，Lowa电子市场允许人们购买份额下注奥巴马或者麦凯恩获取最后的大选胜利。如图9.10所示，奥巴马的价格显示为实线，麦凯恩的则是虚线。你可以看到，随着竞选活动的开展，人们对谁将最终获胜的信心是波动的，但是到了大选前的前一天，奥巴马当选的概率达到了90%，在最终投票之前，预测市场对结果的预判基本上已经确定了。

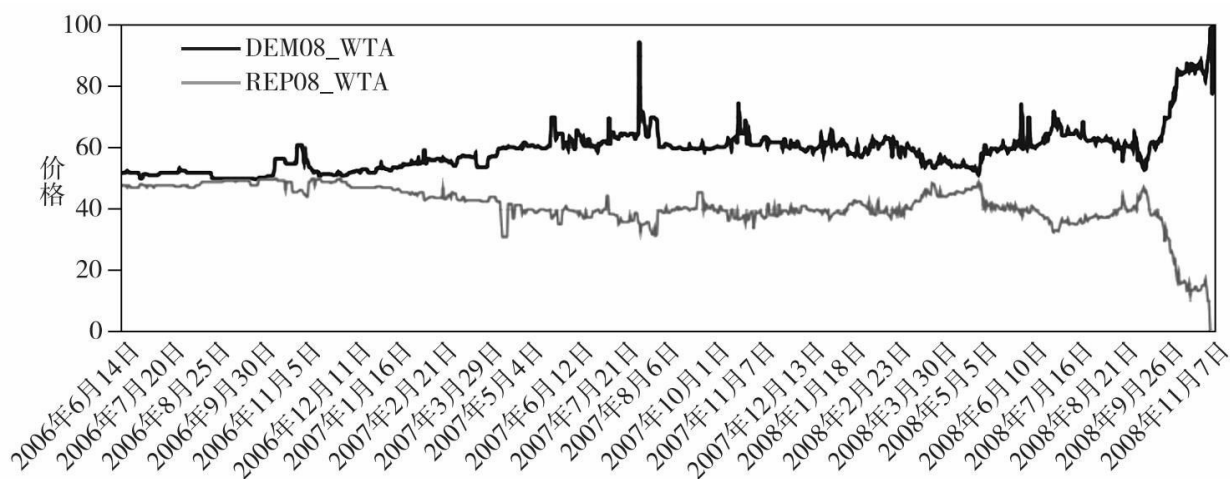


图9.10 预测市场份额

注：对于2008年美国大选预测份额的价格走势图。

资料来源：Lowa电子市场



预测市场的力量

经济学家对预测市场普遍非常热情，关系到预测未来事件的相关信息通常都是比较分散的，由于预测市场提供了一个平台，每一个参与者都可以利用他们的相关知识获利，因此它形成了一个非常好的可以汇聚这些信息的机制。在恰当的经济模型中，股票的市场价格可以被解读为最终结果发生的概率，虽然真实的预测市场还是会存在偏差。根据经验来看，预测市场比类似于投票调查和专家论坛之类的其他预测方法更加准确。

然而，预测市场还是面临很多合规性方面的不确定性和障碍，在2013年碰到合规性问题并被关闭之前，Intrade是美国最受欢迎的在线预测市场。许多经济学家对此很失望，因为他们觉得我们损失了一个非常有价值的可以揭示未来的社会性工具。

去中心化的预测市场

如何建立起一个去中心化的预测市场？我们必须将几个重要的任务去中心化。我们需要一个方法来搜集和发放资金，以使这个预测市场能够建立；我们还需要一个方法来确保执行正确金额的资金发放；我们特别需要一个去中心化的仲裁机构，仲裁是一种流程，用来判决哪个结果是真正发生的。大多数的体育比赛和国家选举，最后结果都显而易见，谁赢谁输，一目了然，但还是有许多灰色地带。我们还需要把下单登记系统去中心化管理，其实就是让参与方直接找到交易的另一方。接下来，我们将按顺序来讨论这些挑战。

让我们来设计一个假想中的被称为“未来币”（Futurecoin）的另类币，专为预测市场所用。我们需要设计一些交易类型实现专为预测市场而设的功能，如图9.11所示。

CreateMarket (event_id, arbitrator_key, num_outcomes)
 创造一个预测，明确仲裁者和参数

BuyPortfolio (event_id)
 为每个未来币的结果购买一份赌注

TradeShares (...)
 将赌注转化为未来币

SellPortfolio (event_id)
 将每个未来币的结果兑现赌注

CloseMarket (event_id, outcome_id)
 通过将特定情境的押注所得转入一个新完成的未来币，并注销所有其他情形的赌注，
 来结束特定预测市场
 (outcome_id 是一个介于 1 和该特定输出 num_outcomes 数之间的整数)

图9.11 未来币中的新交易类型

注：未来币是一个实现了去中心化的预测市场的假想的另类币。

CreateMarket指令允许任何用户制造出一个针对任何事件的预测市场，然后授权一个特定的仲裁者（也就是一个公钥）来宣布这个事件的结果，以及一系列可能的结果。event_id是一个任意的字符串，可以把不同的交易关联起来指向同一个市场。未来币既不关心event_id特指哪个实际事件，也不关心结果是什么，当然在系统里也没有办法来具体定义。用户必须保留这些来自市场创建者的信息（通常这些创建者也是仲裁者）。我们会谈到这个仲裁机制的不同选项。

支付和清算

利用这个BuyPortfolio指令交易，你可以对不同事件的预测组合进行投资下注。以未来币作价，你可以购买每个事件可能发生的预测结果。比如，我们下注2014年的世界杯，32个参赛队都有可能赢。你可以用一个未来币购买32个份额，每个队一个份额——因为最终只有一个队会赢，这些份额的总价格就是一个币。任何一个参与者都可以单方面地

创建一个BuyPortfolio指令而无须一个对手交易。这个交易实际上是利用用户提供的未来币的消耗，以此制造出一个新的份额输入，并分派给每一个可能发生的结果。还有一个交易类型叫作SellPortfolio，你可以卖（或消耗）每一个对应不同的结果的份额，以此赎回一个未来币。未来币和每一个结果对应的份额可以进行互换。

你可以用份额来换未来币，只要可以找到交易对手，你也可以用一种份额去换另一种份额。下面的案例就更加有趣了，你可以用一个未来币购买每一种可能发生的结果的份额，然后把那些你认为不太可能发生结果的份额的卖掉，对于那些你认为没有什么机会获胜的球队，你可以把相对应的份额卖给其他对此有兴趣的人。一旦你做了这些，你的投资组合就不再是每个队均分的，你也就不能再自动赎回一个未来币了，取而代之的是，你必须等到最后的结果出来之后才能赎回你的份额——如果你所押的球队没有最终获胜，你可能什么都拿不回来。另一方面，你也可以直接从交易中获利。你可以购买一个平衡的投资组合，等待价格变化，然后出售所有的份额以换回更多的未来币，这些未来币可以用来和比特币或者其他货币进行兑换。

预测市场的仲裁

如何用去中心化的方法来实现仲裁呢？如何做出判断并宣布胜者和定价，然后胜者可以赎回他们所赢得的份额？最简单的系统就是找一个信得过的仲裁员，也就是上面所说的CreateMarket。任何参与者都可以发起组织一个市场，在这个市场里他就是仲裁员（或是指定某人为仲裁员）。他们可以创建一个交易，然后宣布发起组成了一个市场去预测世界杯的比赛结果，他们会决定谁是最后的获胜者，如果你相信他们，你就可以接受他们在CloseMarket交易上的签名作为最后判决的依据。

就像其他的市场一样，我们可以想象，经过一段时间后，有些实体

慢慢地建立声誉并成了可信任的仲裁者。然后它们就会主动维护它们有价值的声誉并做出公正的仲裁。但是，一旦潜在的获利大于其声誉价值，就会存在风险，也就是它们有可能会去操纵一个预测来获取巨额收益，这对预测市场而言是非常危险的。举例来说，在世界杯的预测市场里，即使阿根廷队事实上输掉了比赛，但是仲裁者还是有可能宣布阿根廷队获胜。如果仲裁者自己买了大量的阿根廷队获胜的份额，他可能会通过操纵这个结果赢足够多的钱，而不在乎毁掉他的名誉。

我们可以有一个更加去中心化的仲裁系统吗？一个选择是设定多个仲裁者，然后基于多数人的决定做出判决，或者基于投票结果——要么由所有在市场上拥有份额的用户进行投票，或者由加密数字货币的矿工进行投票，这些投票方案通常也会要求对投少数票的人进行相应地惩罚。但这些方法都有很多问题，所以我们也不知道它们在实际运用中是否可行。

现实是复杂的。除了仲裁者可能作假的问题之外，事件结果的判断也可能存在争议。我们最喜欢的一个案例就是2014年的超级碗比赛，超级碗上有一个传统，胜利的球队会将一桶佳得乐（Gatorade）饮料倒在他们主教练的头上。人们想要去对获胜球队用来庆祝的佳得乐的颜色进行预测，这种预测市场由来已久。在2014年，预测结果包括黄色、橙色和其他佳得乐饮料所有的颜色。但是在那一年，一个前所未有的结果出现了，很难去决定最终的结果是什么。当海鹰队（Seahawks）获胜的时候，球员们把一桶橙色的佳得乐倒在了主教练彼得·卡罗尔（Peter Carroll）的头上，仅仅过了一会儿，另外一些球员又倒了另外一桶黄色的佳得乐。

如果你主持了这么一个预测佳得乐颜色的预测市场，你会怎么处理这个情况？最终结果应该是橙色，还是黄色，还是两个都算？实际情况是，好几个体育博彩服务提供商为了保持自己的声誉，即使他们因此而损失一些金钱，但为了获取客户对他们的信任，还是决定支付奖金给所

有预测橙色和黄色的用户。

当然，在一个去中心化的市场里，这种做法并不容易，因为你不可能无中生有地创造出更多的资金去支付两种结果的赢家，很可能是仲裁者让预测橙色和黄色的双方平分奖金，最终这两种份额的价格都会变成0.5而不是1.0。为了避免这种复杂情况，你可以一开始在合约里定义清楚，但是你不可能确保你能考虑到所有的可能性。这个案例让我们深刻地意识到，仲裁是个社会问题，通过技术手段是无法完美地解决这个问题的。

实时数据供给

仲裁这个概念引导出一个更加广义的概念：扩展虚拟货币的功能来宣告现实社会里的事实。我们称之为实时数据供给。一个典型的预测市场的事件的事实，比如谁赢了选举、某只股票或者某个大宗商品的当天价格或现实世界里有价值的数据。只要比特币里有了这些数据，脚本语言就可以将其作为输入。比如，一个脚本可以将现货金属铜的价格加载在堆栈里，然后据此价格做出决策。[\[1\]](#)

只要存在一个值得信任的实时数据供给，我们就可以对体育比赛结果或是期货市场的价格进行预测投资和自动结算。预测市场只是其中一个应用而已。你可以通过对相反的两个结果都进行预测投资，以实现在你的投资组合里加入风险对冲。你还可以派生出一些金融衍生产品，比如目前金融市场上常见的远期合约和期货合约。如果这些都能通过比特币来实现，岂不是更好？

我们可以把如何在比特币（或是其他另类币）里用技术手段来表现现实社会事实这个问题，和我们如何建立对数据供给的正确性的信心这个社会问题分离开来。

一个聪明的把数据供给编码到比特币的方法叫作现实密钥(reality keys)。在这个系统里，仲裁者制造出一对密钥，并用该密钥对他们所感兴趣的所有事件的所有结果进行签名。一个密钥代表“是”，另一个代表“否”。他们在注册登记事件的时候先发表公钥，然后当结果确定的时候，再发表那一对密钥里的私钥。如果爱丽丝和鲍勃共同对一个事件进行预测，他们可以把各自的保证金发送到一个比特币输出，爱丽丝可以使用她自己的私钥和“是”这个密钥进行联合签名以提取这个奖金，鲍勃可以使用他自己的私钥和“否”这个密钥进行联合签名提取。这就很好地实现了公正地使用数据供给作为脚本输入的目标，使得上述预测保证金的应用得以实现。值得注意的是，仲裁者不需要知道，也无须参与到爱丽丝和鲍勃之间的特定预测保证金中去。

交易委托

预测市场的最后一个重要环节是一个去中心化的交易委托，这也是一个通用概念，如果能实现，将会使很多的应用设想变为可能。交易委托是什么呢？在一个真实的预测市场里，或者是大多数金融市场里，并没有一个统一的市场价，通常在交易委托中会有买入价（bid）和卖出价（ask）两种，买入价是指愿意购买份额的参与者所出的最高价，卖出价则是愿意出售份额的参与者所出的最低价。通常卖出价会大于买入价（否则市场就会对此进行撮合，至少其中的一个交易委托将不会出现在列表中）。一个想要购买份额的参与者可以立刻以卖出价购买，而一个想要出售的参与者则可以立刻以买入价出售，这个交易被称为“市价委托”，对应于“限价委托”——交易委托被设定为一个特定的价格挂在交易委托列表中，这些交易委托将会按照限定的价格（或者高于限定的价格）执行。

通常这是由一个中心化的交易委托服务提供商（通常是一个交易所）来实现的。但问题是，就像许多中心化的服务所面临的问题一样，

如果这个交易所不诚实的话，它可以通过损害用户的利益来获利。比如，一个交易所收到了一个买单，它们自己可以先在最好的卖出价的时候下单买入，然后马上再在高位卖出，赚取中间的差额。这也叫作预先交易（frontrunning），指的是交易商利用得知客户买卖证券动向的机会，抢在客户发出买卖指令之前为牟取利益而进行交易的违规行为（例如在股票大量交易前，在期权或期货市场进行相应交易），这是一种金融犯罪行为。中心化的交易委托需要执法部门来监管，来防止这种预先交易的行为，以确保系统诚信的公信力。

在一个去中心化的交易委托里，我们不能依赖强有力的执法部门。但还是有一个较好的解决方案：我们不再将预先交易称为犯罪，然后再想办法去防范，我们称之为一个特性。这个想法是，任何人都可以通过广播交易的办法把限价委托提交给矿工，只要买入价比卖出价高或者相同，矿工就能够撮合两个交易。这个矿工只需把两者之间的差额留下作为交易费即可。这样一来，矿工就没有动机去做所谓的预先交易，因为与此相比，预先交易不可能赚得更多。

这是一个很简练地建立去中心化的委托交易的办法。其最大的缺点是交易者必须支付给矿工费用。为了避免支付这种交易费，交易者们可能会提交偏向保守的交易委托，不会在开始时就透露他们愿意成交的最高或者最低价位，这会使得市场变得不是很有效率。我们现在还不知道，这种让矿工撮合交易的交易委托方法在现实操作中是否可行，但看上去这是个不错的主意。

总结一下，现在比特币可以作为很多种应用的平台，但对于某些应用，比特币也没有更好的发展了，比如，对于实现一个安全的去中心化的预测市场，或者是一个去中心化的交易委托系统，比特币并未提供所要求的全部特性。但假如我们从头开始，忘掉硬分叉或是软分叉，忘掉对比特币增加新功能所遇到的挑战，那又当如何呢？自2008年比特币面世以来，我们对比特币有了越来越多的理解和认识，为什么我们不可以

设计一个全新的更好的数字货币呢？

我们将在下一章讨论已经尝试这么做的另类币概念，我们将会探讨所有有前途的想法以及开发一个全新的加密数字货币所面临的挑战。

延伸阅读

我们看过的两种文件的项目材料和说明书，可以参与交易对手条款说明。您可以通过如下网址阅读：

<https://github.com/CounterpartyXCP/Documentation/blob/master/Development>

OpenAssets Protocol可通过如下网址阅读：

<https://github.com/OpenAssets/open-assets-protocol>.

我们描述过的安全多方抽奖协定（The secure multiparty lottery protocol）可以参阅如下论文：

Andrychowicz, Marcin, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. “Secure Multiparty Computations on Bitcoin.” Presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, 2014.

您可以通过如下网址阅读：

<https://eprint.iacr.org/2013/784.pdf>.

经济学家们预测市场的能力的研究，请参阅如下论文：

Wolfers, Justin, and Eric Zitzewitz. “Prediction Markets.” Paper w10504. Cambridge, MA: National Bureau of Economic Research, 2004.

Arrow, Kenneth J., Robert Forsythe, Michael Gorham, Robert Hahn, Robin Hanson, et al. “The Promise of Prediction Markets.” *Science* 320, 2008.

我们讨论过的预测市场设计的相关内容，可以参阅如下论文（由多位作者合著）：

Clark, Jeremy, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, and Arvind Narayanan. “On Decentralizing Prediction Markets and Order Books.” Presented at the Workshop on the Economics of Information Security, State College, PA, 2014.

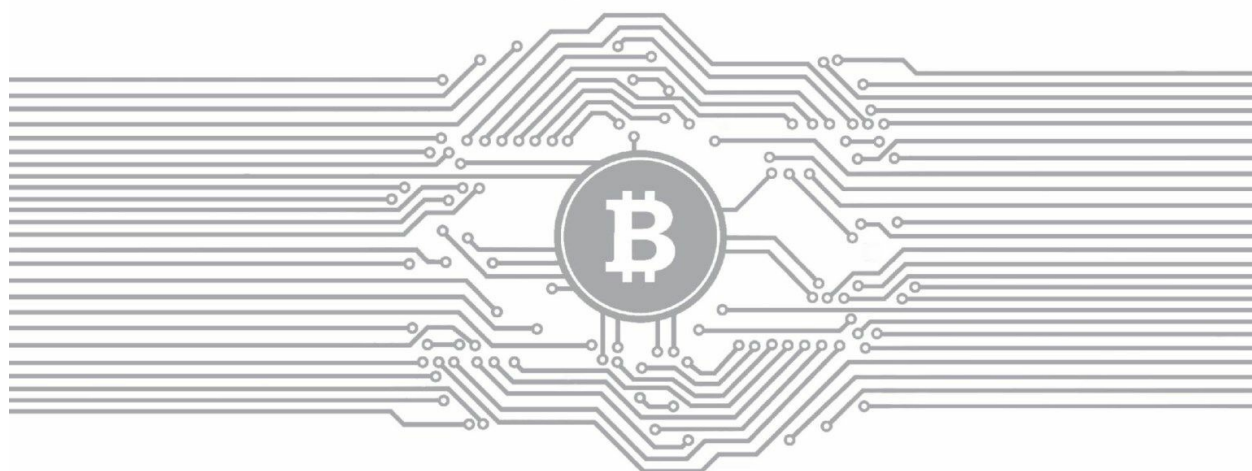
您可以通过如下网址阅读：

http://www.jbonneau.com/doc/CBEKMN14-WEIS-decentralizing_prediction_markets.pdf.

[1] 技术细节请参阅第3章相关内容。——译者注

第10章

另类币和加密货币生态系统



比特币，尽管是非常重要的组成部分，但它只是范围更广泛的数字生态系统中的一种，该生态系统的其他货币也与比特币相似，我们称之为**另类币**。本章中，我们将探讨另类币及**加密货币生态系统**（cryptocurrency ecosystem）。

10.1 另类币的历史和诱因

2009年1月，比特币诞生。2011年年中，还未到两年，第一个基于比特币的衍生货币——**域名币**就出现了。2013年，另类币出现爆炸式增长，迄今为止已有数百个（见图10.1）。由于没有明确的统计标准，我们无法给出确切的数字。举个例子，如果有人宣布创造了一种另类币，可能也公开了源代码，但无人挖矿也无人使用，这种货币是否需要纳入统计范围？此外，有些另类币，在其诞生初期是有人使用的，但后来很快就无人问津了，这类货币是否也需要纳入统计范围？

而且，我们也不清楚如何区分另类币和传统数字加密货币。早在比特币出现之前，就有多种数字加密货币的方案和系统，这些货币并不能称作另类币。许多另类币借用了比特币的概念，它们通常是直接复制其基础代码或是使用部分代码。有些只对比特币做了极小的改动，例如只改变一些系统参数值，保留比特币开发者后续所做的所有变更。截至目前，所有已知的另类币都是从一个新的创世区块开始，都有自己独特的交易历史，而不是从比特币历史交易记录中的某个区块进行分叉，进而演化出自己体系的。为了研究和学习，我们并不需要另类币的精确的定义，而是把将所有在比特币之后诞生的加密货币笼统地称为另类币。

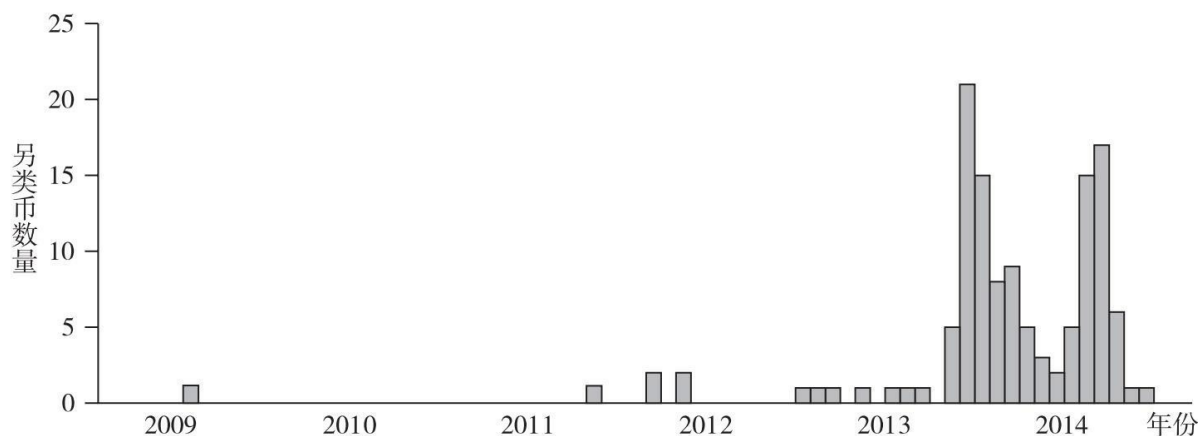


图10.1 每月创造的另类币量

注：仅指通过创世区块创建的另类币。

我们将简要提一下非另类币系统，如瑞波公司（Ripple）和恒星公司（Stellar），它们属于第2章中所介绍的传统分布式共识协议。这类系统为了达成共识，模型中每个节点都有自己的标记并且需要知道其他节点的标记。当然，比特币建立共识的模型与此截然不同。在瑞波公司和恒星公司中，共识协议支持支付清算网络并且在每个体系中有其自己的货币。尽管这些特性和另类币类似，但在本书中并未将它们作为另类币考虑。

发行另类币的原因

每种另类币都有自己的故事。一种另类币之所以存在，就是因为它有别于其他另类币的特点。最简单的情况下，一种另类币只是修改比特币内置的参数，比如修改区块的平均时间间隔、区块大小限制、创造回报的计划和货币的通货膨胀率等。

当然也有更复杂的技术上的差异，这种情况更有趣。例如，可以对脚本语言进行扩充以增加交易种类和安全属性，可以采用与比特币完全不同的挖矿方式以及**共识算法**（consensus algorithm）。

有时，为了支持一个主题或者社区，通常是需要给社区中的成员赋予一个特定的角色或权限，就会有一种比特币被创造出来。本章将在最后的部分研究此类相关案例。

如何创建一个另类币

我们首先考虑一下另类币在创建过程中及创建后所涉及的内容。正如前文提到的，创建一个另类币就是建立一个全新的参照体系，最常见就是通过复制修改现存的成熟另类币或者比特币本身。最容易的部分就是加一些技术特色或者修改一些参数使之更好用。曾经有一个网站 coingen.io，只收取一些费用，就会自动产生一个另类币。你只需要自己设定各种参数，比如区块产生的平均时间、需要的工作量证明算法、另类币的名字以及3个字母的货币代码和标志。完成设置后，只要轻轻点击鼠标，就能下载一份根据你的需要修改的比特币源代码，你就拥有了自己的另类币，接下来你就可以和别人马上开始运用这个另类币了。另类币最困难的部分在于如何让别人逐步接受并使用你的另类币。通过复制并修改源代码，你可以对外发布新的另类币，在刚诞生时，没有人会使用这个货币，由于没有人想拥有这个货币，因此它毫无价值，又由于没有挖矿的人，它也不安全。本书第7章，我们介绍过比特币系统的利益相关者：开发者、矿工、投资者、商家、客户和支付服务商。最终，为了让你的另类币形成规模，你需要吸引这些参与人加入这个货币的生态圈中。

另类币的这些相关群体都是非常重要的，而且它们相互关联，这与创建并推广一个平台非常类似。比如，创建一个智能手机操作系统，就需要用户、设备制造商、手机软件开发者和其他重要的利益相关者共同参与，同时每个角色都需要群体中的其他人的参与。

在另类币中，吸引矿工对另类币来说特别重要，因为如果没有足够

的哈希算力做支持，双重支付和复制修改代码就很可能发生，另类币的安全性就无从谈起。事实上，这种货币可能会彻底崩溃，本章10.4节中将会讨论“另类币夭折”（altcoin infanticide）。没有一个简单的方法可以吸引大家接受并逐步推广使用另类币，但是通常来说，当矿工感觉到货币回报值得他们付出时，他们就会加入。为了吸引矿工，很多另类币都给早期矿工比较丰厚的回报。比特币显然是最早采用这种策略的，后来很多另类币采用了更加激进的激励措施来吸引早期矿工。

而最困难的工作，是让一个社区的人相信这个另类币有价值。正如我们在第7章讨论过的，即便对比特币来说，我们也不是特别清楚这个过程是如何自举的。这依赖仙子效应，从而实现自我增强，让人们相信它有价值的过程是如何实现的。这就回到我们一开始提到的，另类币需要有一个好的故事，才能让人相信这个新的另类币将来会有价值，或者是相信其他人会认为这个有价值。如果一个社区对获取另类币感兴趣，矿工就会参与进来。^[1]只要价值被认可，其他重要的元素就会显现，比如在交易所交易以及从开发区块链的工具，到游说团体开发的各种辅助设施和服务。

拉高出货骗术（pump-and-dump scams）

当一种另类币的创始人成功地促成一个活跃的货币社区和一个真正在运作的交易市场时，他们就会变得非常富有。几乎可以肯定的是，他们拥有很多这类货币。这种货币可能来源于，在系统运行最初，哈希算力还不是很高的时候所挖的货币，或者是类似接下来要讨论的，在还未挖矿之前获得的预先分配的货币。一旦另类币的交换价值提高了，创始人就可以选择卖掉他们的货币。

一夜致富的可能性，极大地吸引了有雄心的创业者和风险投资基金，毫不意外地也吸引了骗子。事实上，我们很难区分骗子和创业者。

骗子可能会使用各种方法，来夸大一种另类币的潜在和未来收益。他们可能会炒作它的技术优点，伪造底层支持的假象，在市场上推高另类币价格等。

事实上，甚至连非创始人都可以设计这样的骗局。他们可以先买入大量还未出名的另类币，然后说服大众相信该货币还有未实现的增值潜力（也就是“拉高”）。如果成功地拉高了货币的价格，他们就可以通过卖出获利（也就是“抛售”）。此时，很多理智的投资者可能会意识到这是个骗局，然后币值出现断崖式下跌，导致很多当初购买的人最终血本无归，只剩下毫无价值的货币。这种拉高出货的骗局，在操纵不知名的低价股票的主流金融业务中很常见，在另类币的发展早期也很普遍，那时候用户热情高涨，投资者也无法分辨到底哪一种另类币是真正具有创新性的，哪一种是靠噱头和推广，但实际是毫无真正价值的。这也导致，截至目前，用户和投资者都厌烦了另类币。

初始分配

在比特币体系中，货币只能以挖矿的方式分配给用户。但是在其他另类币体系里，出于各种考量，除挖矿以外，开发者们还使用其他方法对货币进行初始分配。

开发者可以预先分配货币，也就是说，先预留一部分货币给自己或者其他特定团体（比如预留给开发该货币的非营利性组织）。用这个额外的收获，去激励开发者花费时间精力去创造和激活一个新的加密货币。有时候，也可能会采取更激进的激励方式，即可以对货币进行预售，也就是把这些货币预先卖给其他投机者，换取比特币或者现实中的货币。这有点像投资初创企业：如果投资的另类币成长起来，投机者就会获得大量财富。

寻求各种预分配方法的另外一种动机是，确保早期的货币拥有者来自多个社区，并且他们与货币成功的利益相关。如果矿工太过集中，就会造成资产持有过度集中，这不利于货币的发展壮大。一种比较聪明的分散所有权的做法，就是把另类币发给现有的比特币用户。

在技术上如何做到这一点，即让比特币用户可以自动地分配，并拥有另类币？一种办法是通过第3章谈到过的“销毁证明”：用户只要证明他们销毁了一定比例的比特币，就能要回一个单位新的另类币。用户需要在销毁的时候提供数据证明，比如特殊的字符串来识别某个另类币，这样就可以说明他们销毁比特币的目的，就是为了获取这个新的另类币（见图10.2）。

通过“销毁证明”来分配另类币，也叫作“单向挂钩”或者“价格上限”。另类币可以一对一地对比特币，并不意味着两者价值相同。这样的配对，确保另类币最多值1个比特币。因为，1个比特币可以换1个另类币，但是反过来不行。

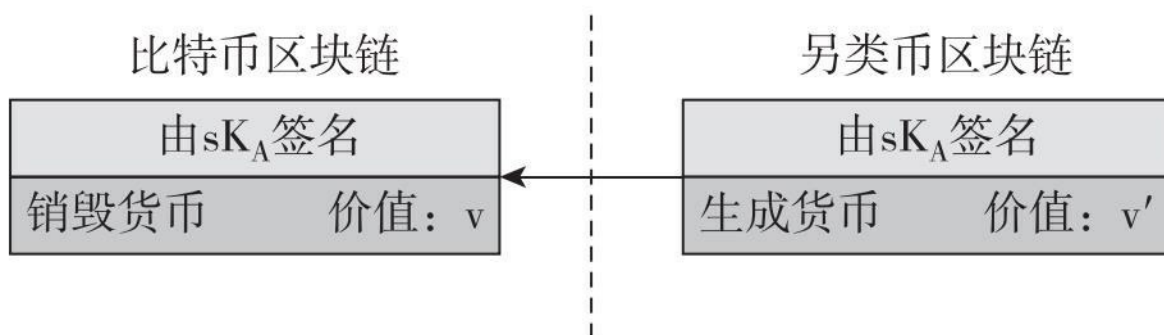


图10.2 通过“销毁证明”分配另类币

注：另类币提供一个以比特币操作为输入的生成货币（GenCoin）的指令。生成货币的签名用到的私钥，和签销毁证明的私钥是一样的（签名的机制也一样）。这样就能保证，销毁比特币的同一个用户，同时创造了新生成货币。如果兑换比例是1：1，那么另类币的价值 v' 不大于比特币的价值 v 。

也可以有一些相对没那么复杂的做法：要求用户提供拥有比特币的证明，但无须销毁比特币，也以获得新币。具体来说，另类币体系会指

定一个比特币区块高度（也许刚好就是另类币诞生时的长度）。在这个高度的区块里，任何人拥有还没花掉的比特币，就可以按比例得到同样数量的另类币（见图10.3）。通过这种方式，比特币和另类币的价格就无须固定，毕竟比特币并没有通过销毁证明来“转换”成为另类币。

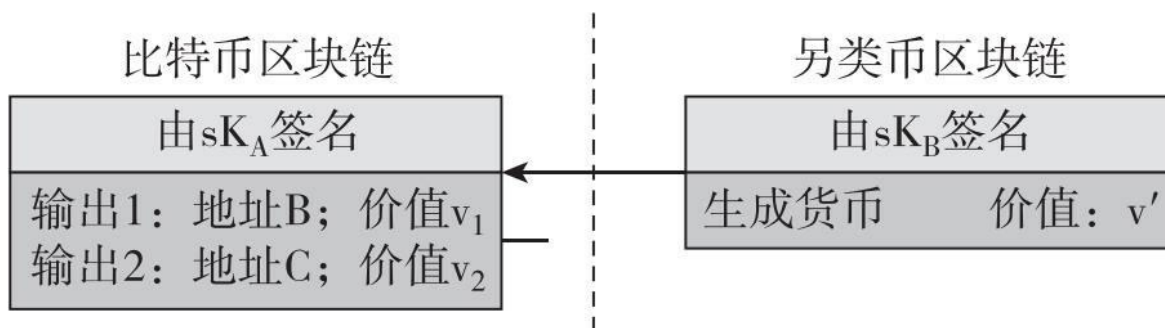


图10.3 通过证明比特币的所有权来分配另类币

注：生成货币的输入，是特定区块高度下一个或者多个没用过的比特币交易输出。就像正常的比特币操作一样，这些都是通过控制未使用比特币的私钥来进行签名认证的。图中的比特币交易有两个未用过的交易输出，分别为特定高度区块链中的B和C地址。B地址的用户换了另类币，但C地址用户还没这么做。假设汇兑比例是1：1，新另类币的价值为 v' ，那么 v' 一定不能大于B的比特币价值 v_1 。

当然，为了实现这种分配，另类币的矿工也必须时刻了解比特币的区块链。另类币必须明确什么才算认定的比特币交易。一种选择是要求固定的确认次数，比如6次。另外一种选择是，在每个另类币的区块中加入最新比特币区块。这样，比特币的交易立刻可以在另类币体系里使用，而不需要等待确认。这就类似在比特币体系中，交易的输出可以在自身或者下一个区块中使用。我们将在下一节讨论**共同挖矿**（merge mining），一种把比特币和另类币区块链链接起来的方式。

最后一种方式是，把已经分配好的货币捐赠出去，这也是扩大货币用户多样性的一种办法。一种方式是支付小费：很多服务允许赠送小费给电子邮箱或者社交媒体账户，这多多少少可以促进接收者了解并参与到这个货币体系中来。接受方收到信息，得知他的托管账户存有小费，然后通过认证邮件地址或者社交媒体账号可以取得这些小费。当然，为

获得这些小费，他们还需要安装钱包软件，或者采用其他方式。另外一种可以称作“水龙头”捐赠方式，即任何访问特定网站并输入邮件地址的人，都可以获得一小部分另类币。

[\[1\]](#) 尽管当币种升值快于挖矿的速度时，可能会有风险。——译者注

10.2 几种另类币的详细介绍

接下来，我们重点介绍几个最早的另类币。

域名币

本书已经介绍过比特币的区块链是一种安全的全球数据库，其对写入的数据具有防篡改保护，并且是永久的。那么是否可以修改比特币的设计，来支持其他安全的全球数据应用（比如域名系统）呢？

为了使这个数据库在非货币方面的应用更加有效，我们首先需要明确几个基本原则。第一，把录入的数据视为域名或数值对（`name/value pairs`），域名是全球唯一的。这就可以使任何人去寻找可映射到域名的数值，就像哈希链表或者有主索引的数据库一样。为了确保域名的全球唯一性，如果域名和数值对与以前录入的相同，则将其视为对旧数据的更新而非新的数据。

第二，只有首次录入某个域名的使用者，才有权限更新这个域名。这很容易实现，比如可以把每个域名与比特币地址联系起来，且规定必须用这个地址的私钥，才可以对更新交易签名。

比特币可以实现上述功能，正如第9章中所述，可以把比特币作为只有增添功能的日志来构建叠加货币。由于可以直接把这些协议写入规则中，其他另类币更易于实现上述功能。而且，一旦矿工执行了这些规则，这些规则就是不可改动的，而且不需要每个使用者（如全部节点）自己检查并判断在受到侵犯时该如何处理。它甚至可以实现类似SPV形式的验证：一个轻量级的客户端可向运行全节点功能的服务器提交一条

查询（如查域名），服务器则会返回这个域名项的数值以及相关证据，用以证明返回的数值是数据库中最新的数据。

上文简要介绍了域名币。这是一个全球的域名/数值商店，在这个体系中，每一个用户都可以注册一个或者多个域名（需要一定的费用），并且可以更新他们拥有的域名的数值。用户同时也可以把拥有的域名转给别人。事实上，由于域名转让与货币转让交易不可分割，你可以在把域名转给别人的时候，获得几个单位的域名币。通过这种方式把域名卖给从未谋面并且未建立信任关系的人是安全的。虽然截至2015年，域名币还无法支持安全简单的客户端，但是支持这个扩张功能的提议已经被提出来了。

域名币的目的是提供一个去中心化的域名系统DNS，在DNS数据库里，名字即域名，数值对应IP地址。目前还无法在普通浏览器里默认使用域名币，但是通过下载相关插件，这个插件就会在域名币的注册系统而非传统的DNS中查找IP地址，这样，用户就可以在像火狐（Firefox）或者酷睿（Chrome）此类的浏览器中访问如example.bit这样以.bit结尾的域名了。

域名币不仅在技术上而且在历史地位上都是很值得一提的。它诞生于2011年4月，仅比比特币晚两年，是第一个被创造出的另类币。其特点是共同挖矿，本章10.4节将就此做进一步讨论。

截至2015年，域名币并未被广泛使用。大部分的注册域名都被一些投机者抢先注册，他们希望通过卖域名获利（现实远未如此）。支持域名币系统的人认为，不应该让现有DNS体系将互联网核心组成部分的控制权，过多地交由单一机构来管理。可以想象，这种观点在比特币社区中也很流行。但是主流用户对于用其他方式来替代DNS并不热衷，因此，域名币这种杀手级应用无法普及。

莱特币

莱特币（Litecoin）诞生于2011年，在域名币之后。在过去的几年里，无论是从综合流行程度或是用户基础看，莱特币都是另类币中的领头羊。它也是被模仿修改最多的货币。事实上，莱特币被模仿修改的次数超过了比特币。

莱特币和比特币在技术上的主要区别是：莱特币用的是第8章讨论过的基于Scrypt算法的刚性内存解谜（memory-hard puzzles）。当莱特币出现的时候，比特币的挖矿还在GPU时代，所以当时莱特币使用刚性内存解谜，目的是替代GPU。一开始发行时，还可以用CPU在莱特币中挖矿，虽然那时候比特币早已无法使用CPU来挖矿。但是后来，莱特币也无法阻止挖矿的层层升级，从CPU到GPU再到ASIC。每次莱特币挖矿的升级，都比比特币花费的时间更长。其中原因，也许是因为莱特币的谜题，用硬件去解更难，或者由于莱特币币值交换比例较低，使得矿工缺乏动力。

不管是何种原因，从CPU升级到ASIC，就挖矿功效的改进效果来看，莱特币与比特币类似。从这点来看，莱特币并没有达到原先设计的目标：通过维护CPU矿工社区，创造出一个用CPU挖矿的分布式体系。但是，重要的是，这个理念虽然失败了，它依然吸引并保持了众多的追随者。如今，莱特币已经改变了其说法，声称由于其并非采纳ASIC，因此其初始分配更加公平。

莱特币也做了一些小的参数变更，比如莱特币的区块增长会比比特币快4倍，也就是每2.5分钟产生一个区块。其他方面，莱特币都尽可能借鉴比特币。甚至莱特币的更新都跟随比特币，比特币一有任何补丁或者更新，莱特币会同时采用。

狗币

狗币（Dogecoin）也许是迄今为止故事最精彩的另类币。它诞生于2013年年末，其突出的特点不是技术（它是莱特币的翻版），而是社区价值体系：小费、慷慨和非严格的加密货币。它的名字来源于神烦狗（Doge），一只有趣的在互联网流行的日本柴犬（见图10.4）。狗币团队发起过好几个有趣而且成功的广告宣传活动，比如赞助美国纳斯卡车赛（NASCAR）车手，让狗币的图案遍布全车。他们还集资了3万美元，资助牙买加国家雪橇队参加2014年冬季奥运会。有趣的是，这和90年代的电影酷跑（Cool Running）的故事情节如出一辙。



图10.4 狗币的其中一个标志

注：卖点是其有趣幽默，而不是其技术创新。狗币标志，版权为2013~2014年狗币开发者。

由于狗币社区的慷慨大方、宣传活动的推广，加上神烦狗形象在互联网的流行，狗币在2014年一度大受欢迎。很多用狗币的人，之前都不知道什么是加密货币，他们也不需要知道狗币比别的货币好在哪里，就

可以主动参与并推动狗币的发展。狗币的成功，说明一个货币的流行也可以通过非技术的方式来实现。遗憾的是，就像很多互联网热点一样，狗币的风靡程度目前已逐渐减弱，其汇兑比率也随之大幅下降。

10.3 比特币和另类币的关系

我们可以用一系列的参照标准，来比较各类不同的另类币的相对规模和影响。

另类币比较

资本市值

传统上来说，资本市值是评估一个公众公司的简单方法，把公司股票价格乘以总股份即可得出资本市值。在另类币领域里，计算资本市值的方法类似，即用每单位货币的价格（通过用最通用的第三方交易平台取得价格）乘以流通中的总货币数。按照这个标准，截至2015年，比特币的资本市值最大，其占了所有加密货币总和90%多的市值。其他币种的排名可能会经常变化，但是大部分另类币的市值都非常小。

不能过分看重资本市值。首先，资本市值并不等于购买所有流通中货币的总费用。这个总费用可能比资本市值高或者低，因为大量的购买会抬高该另类币的价格。其次，虽然资本市值只考虑流通中的总货币量，但是市场参与者应该会考虑未来新发行货币量对货币价格的影响，这使资本市值的估计更加复杂。最后，甚至真实流通的货币量也是无法准确估计的，因为有些货币的主人也许丢失了他们的私钥，但我们并不知道。

挖矿能力

如果两个另类币用同样的挖矿谜题，那么可以直接对比每个货币矿

工的总挖矿能力。基于哈希谜题的影响，挖矿能力这个指标经常被称为**哈希速度**（hash rate）。比如，**泽塔币**（Zetacoin）用和比特币一样的SHA-256挖矿谜题，在2015年12月，它的网络哈希速度，是5兆哈希每秒(即 5×10^{12} 哈希/秒)。这个数字大约是比特币的十万分之一。如果两种货币用不同的挖矿谜题，比较挖矿能力就很困难，因为谜题需要花不同的时间去计算。而且，专门为某种货币定制的挖矿硬件不一定适用于其他货币的挖矿（包括攻击）。

即便对使用完全相同的挖矿谜题的另类币，我们也可从其随时间而变化的挖矿能力上，得知一些有用的信息。如果是算力的增加，则意味着更多的人加入或者现有参与者升级了更强大的硬件设备；反之，如果是算力的减少，则意味着一些矿工已经放弃这个币种，这通常是一种负面的迹象。

其他指标

有几个其他指标可以用于比较另类币。比如，另类币的汇率变化可以说明其健康程度，当然也可能与其哈希速度变化有关；在第三方交易平台的交易额可以用来测度这个货币的活跃度和公众对它的兴趣程度。然而，有些指标并不一定有用。比如，另类币区块链的交易量就并不能说明什么，因为这有可能是用户在他们自己的账户内通过倒转货币产生的，这些内部倒转甚至可能是自动进行的。最后，我们可以看看有多少商家和支付渠道支持这种货币，因为只有优秀的货币才更可能得到支付渠道的支持。

比特币与另类币互动的经济学视角

比特币和另类币的关系很复杂。一方面，作为加密货币，因为它们都可以用于网络支付，它们相互竞争。如果两种货币提供的功能相近，

采用类似的标准、协议和规范格式，那么最终有一方会占优，这就是经济学家所说的“网络效应”。

举个例子来说，在2000年的中后期蓝光（Blu-ray）和HD DVD展开激烈的竞争，争夺DVD标准的制定者。因为受欢迎的游戏机PS3(PlayStation 3)的主机可以当成蓝光播放器使用，渐渐地，蓝光开始变得更加流行。很多电影制作商也由此更喜欢采用蓝光格式，这也反过来推动了蓝光进一步的普及。随着更多的电影采用蓝光格式发行，更多的用户购买蓝光播放器，进一步导致更多的电影采用蓝光格式。同样，如果你的朋友都用蓝光播放器，你也会买蓝光而不是HD DVD播放器，因为这样，你和朋友互换电影会更容易。因此，仅仅用了两年的时间，HD DVD就成了历史。



谁最终获胜？

早在HD DVD被淘汰之前，就有无数相似的技术标准被竞争者迅速取代，从而暗淡地退出历史舞台，如Betamax模拟磁带以及俄罗斯标准铁路轨道等。因为网络效应，你可能没听过这些被替代的东西。有时候，胜出者是因为其压倒性的技术优势，就如同尼古拉·特斯拉（Nikola Tesla）的交流电网在与托马斯·爱迪生的直流电网中获得的优势一样。然而，大多数时候，失败一方事实上在技术上更胜一筹，比如Betamax磁带就输给了VHS磁带，可见网络效应如此之大，以至于微小的技术劣势可以忽略。

以上的推理说明，即使后面跟随的其他货币在技术上更先进，最终只有一个加密货币会占主导地位（目前看来可能是比特币，因为它是当前最流行的货币）。但如果仅仅只是这样看待货币之间的竞争，那就会过于肤浅，加密货币之间的竞争，之所以不像光盘格式之间的竞争那么

你死我活，至少有以下两个原因：

首先，用户从一种加密货币转向另一种相对容易，服务商也容易接受多种加密货币，这意味着多种加密货币更易于共存和发展。加密货币的这种特性在经济学上被称为较低的转换成本。相反，DVD播放器的转换成本很高，因为绝大多数人不需要两个笨重的播放器摆在家里，如果更换到另外一种播放器，也不容易把已经有的光盘转化为另外一种格式。当然，加密货币之间的转换成本也不是完全没有。比如，用户也许已经购买了一个硬件版的钱包，如果转换其他货币，硬件钱包可能无法升级转化。但是正常来说，转换加密货币并同时使用多种加密货币是很简单的。

其次，正如前面提到过的，很多另类币之所以存在，是有其独特的功能基础的。这些另类币并不只是比特币的替代品。它们和比特币功能有交叉，甚至互补。从这个角度看，可以功能互补的另类币实际上扩大了比特币的用途，而并不仅仅是和比特币竞争。例如，假设域名币成功了，那么比特币的用户在使用比特币的时候，就多了一个选择。

当然，如果把它们之间的关系都理解成愉快的合作共赢，也过于肤浅。一些另类币，比如莱特币，就是想要用更加高效的方式来达到比特币的功能。莱特币的创新功能，其实都可以在比特币体系里实现，或者用相对笨拙的办法来实现（第11章将做进一步的讨论）。支持在比特币体系基础上持续改进的人认为，多种另类币分散了可用哈希算力，从而使每个独立货币不太安全。

相反，支持另类币的人则认为，另类币可以让市场决定什么功能值得拥有、什么系统更加优越等。他们同时还认为，多种另类币系统同时存在的话，可以把任何一个货币系统灾难性的损失控制在一定范围内。他们也指出，比特币开发者高度风险厌恶，不管是通过软分支还是硬分支，加入任何新功能，都是非常缓慢和困难的。相反，在另类币上很容易去尝试新想法。因此，可以把另类币视为比特币新功能的实验田。

实际上，最终结果就是，比特币和另类币的支持者之间既相互竞争也相互合作。

10.4 另类币的夭折与共同挖矿

本节和下节将继续讨论比特币和另类币的技术相关性，而暂时搁置文化、政治和经济因素。

另类币的夭折

截至2015年，比特币的哈希算力让所有任何其他另类币相形见绌。事实上，存在几个势力强大的矿工或者矿池，他们控制的挖矿能力高于所有其他另类币的挖矿能力总和。这样的矿工或者矿池，可以轻松攻击一个小的另类币（如果他们也用和比特币一样的SHA-256挖矿谜题），通过制造废品和大规模混乱，最终毁了该另类币。我们称这种现象为另类币的夭折。

用宝贵的挖矿算力去攻击其他货币，并且得不到明显的金钱回报，为什么会有人这么做？以2012年**盘旋币**（CoiledCoin）被攻击为例：比特币矿池Eligius的总管认为，盘旋币是个骗局，会对整个加密货币的生态系统产生冲击。所以，Eligius将其挖矿资源全部用在盘旋币上，制造出的区块链把盘旋币几天的交易给对冲掉，同时挖了一条很长的空区块链。这造成了其他盘旋币用户无法再使用盘旋币的服务，也就无法再产生任何新的交易。在盘旋币经历了短暂的攻击后，用户放弃了盘旋币，它从此销声匿迹。在这个案例，以及其他类似的另类币夭折的案例里，攻击者都是出于金钱以外的动机而发动攻击的。

共同挖矿

如果一个另类币复制了比特币的源代码但是没有做任何修改，按道理在这个另类币上的挖矿是有排他性的。也就是说，你可以去试图找挖矿谜题的答案从而找到一个有效的区块链，但是只能给另类币或者比特币，不能一石二鸟。你可以把你的挖矿资源在比特币和另类币上做分配，你甚至可以在多种另类币上分配资源而且随时调整配置，但是无法让挖矿资源同时服务于多种货币。

在这种具有排他性挖矿的条件下，网络效应会使很多另类币无法实现自我增强式的循环发展。如果你开发了一个新的另类币并成功说服当前的比特币矿工加入你的另类币体系，为此，他们必须停止比特币的挖矿，也就意味着他们会立刻产生相关损失。因此，他们没有动力加入你的另类币体系，也就意味着你的另类币很可能只有很低的哈希算力，也就很容易被其他比特币矿工攻击并夭折。

是否可以设计出这样一种另类币，它可以允许同时在该币和比特币上进行挖矿？为了达到这个目的，则必须创造出包含比特币和该另类币相互交易的区块链，以使这些交易在两个区块链均有效。设计可使比特币的交易出现在其区块里的另类币，这个并不难，我们可以设计任何想要的另类币的规则。但反过来却很难。如何把另类币的交易放入比特币区块链上？第3章和第8章已经介绍了如何把任意数据放在比特币的区块里，但是这样做会遇到比特币特有的带宽限制，即其数据传输量非常有限。

然而还是有巧妙的办法：虽然不能把另类币的交易内容放进比特币的区块里，但是可以把另类币的交易概要以哈希指针的形式放入比特币区块中。找一个可以在每一个比特币区块里放入一个哈希指针的办法很容易。具体来说，回想一下本书曾经提过每个比特币区块都有一个特殊的交易，称为**币基交易**，也就是矿工创建新的区块所得的比特币奖励。这种交易的**输入脚本**（scriptSig）区域没有任何内容，因此可以用来存储任意数据（当然也不需要对比基交易进行签名认证，因为没有

任何前序交易)。所以在—个共同挖矿的另类币体系里，挖矿的任务就是去计算—类特殊的比特币区块，币基交易的输入脚本区域存有指向另类币区块的哈希指针。

这个区块现在可以身兼二职：对比特币客户端来说，其与任何其他比特币区块没有区别，除了在币基交易中多了一个可以被比特币忽略的哈希值。另类币的用户知道如何解读这个区块：忽略比特币的交易，只看在币基交易中的哈希值所指向的另类币的交易。值得注意的是，这种设计不需要比特币做任何改变，但是需要另类币能够兼容比特币，并且允许共同挖矿。

如果另类币支持共同挖矿，那么我们希望很多比特币的矿工也参与进来，因为这不—需要花任何额外的哈希算力。只需要增加少量的运算资源去处理区块和交易，以及矿工需要知道和了解这个另类币，就能去花费精力来挖矿了。假如25%的比特币矿工的哈希算力同时在挖另类币的矿，这说明，平均25%的比特币含有指向另类币的指针，也就意味着，在另类币体系里，每隔40分钟才能产生—个新的另类币。而更糟糕的是，当另类币还在自我发展，并且只有小部分的比特币矿工参与的时候，产生—个新区块需要几个小时甚至几天，这种局面实在让人无法接受。

有没有办法确保参与共同挖矿的另类币的区块，能按照稳定的速度产生？或者说，我们是否可以设定区块产生的速度或高或低，但与比特币中多少比例的人参与共同挖矿无关？答案是肯定的。奥妙在于，虽然另类币的挖矿任务和比特币—样，但是挖矿的目标不同。另类币体系计算的目标和困难程度和比特币体系中的目标和困难程度都没有关系。就如比特币可以调整其计算目标使每个区块按平均每分钟产生10个的速度—样，另类币也可以调整自己的目标使区块在另类币体系也以每10分钟或其他固定值产生—个。

这意味着，另类币的目标值要远远小于比特币的目标值。部分，甚

至是大部分另类币的区块将不会被有效的比特币区块的指针指引到。但是这并不会带来问题，你只需要把比特币区块链和另类币区块链看成是两个平行并列的数据链，只是偶尔有从比特币指向另类币的指针，详见图10.5所示。在图示的例子中，60%的比特币矿工同时也挖另类币的矿，另类币大约5分钟产生一个。这意味着另类币的挖矿难度系数是比特币的 $60\% \times 5/10 = 30\%$ 。图中40%的比特币区块没有包含指向另类币的哈希指针。

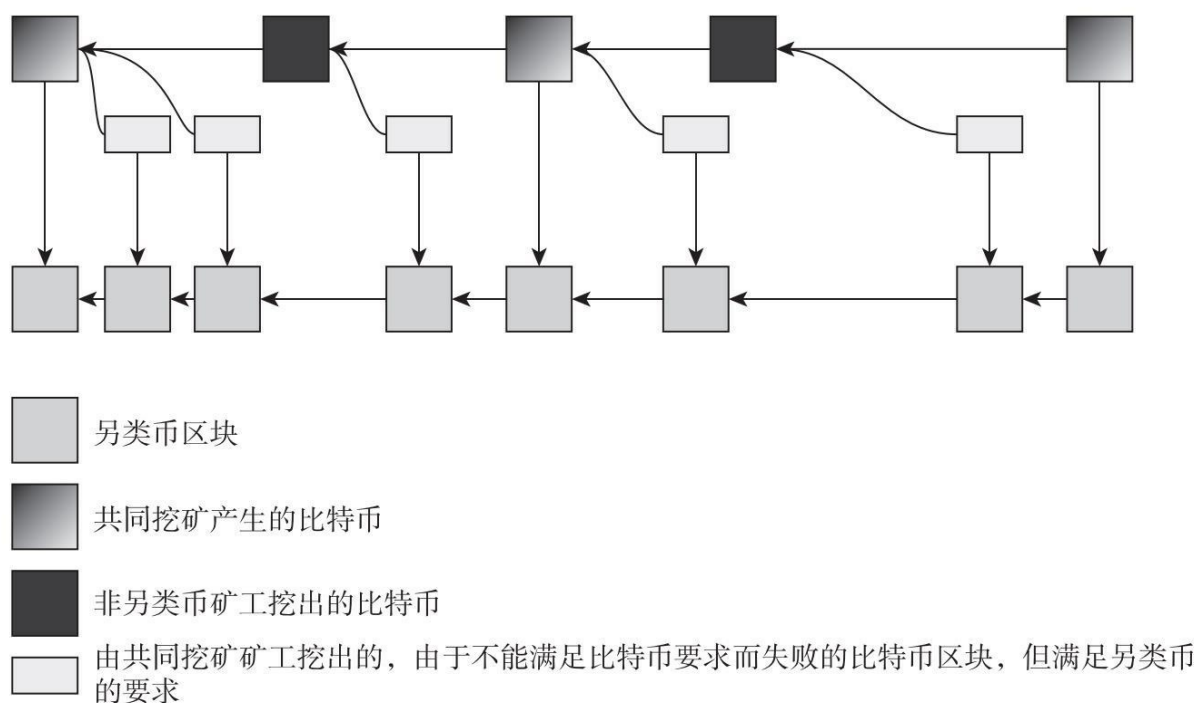


图10.5 共同挖矿

注：图中显示了比特币和另类币的区块链，以及它们之间的相互作用。

相反，每个有效的另类币都是比特币挖矿的结果，但是在所有满足另类币的挖矿算法结果中，只有30%能达到比特币的要求。对于另外70%满足另类币要求却无法达到比特币要求的区块，另类币的网络需要验证这些区块是否真的符合解决挖矿的谜题。最直接的方法是向比特币相邻区块和另类币区块进行广播。更聪明的方法，是只广播比特币相邻区块的标题部分和比特币区域中包含币基交易的二进制证明。

虽然很罕见，另类币的谜题也可能比比特币更难。由于大部分另类币希望产生区块的速度要快于每10分钟一个，这种情况不常见。当然如果希望放慢速度的话，也很容易做到。这种情况下，你就会看到有些矿工挖到比特币，希望这些也能成为另类币，但是部分比特币区块，在另类币网络中，由于达不到更高的难度要求而被拒绝。

最后需要指出，任意数量的另类币都可以同时和比特币共同挖矿，每个矿工都可以自由选择任意另类币共同挖矿。在这样多种另类币组合共同挖矿的情况下，币基交易的输入脚本本身就是一个指向多种另类币的二叉哈希树结构。注意这种结构的复杂性，因为确认包含另类币交易需要确认以下几点：（1）二叉哈希树包含这个另类币的证明；（2）二叉哈希树证明包含币基交易输入脚本，而且里面包含另类币的哈希值；（3）二叉哈希树证明比特币区块或者附近区块有币基交易的输入脚本。

共同挖矿和安全

共同挖矿是一把双刃剑。正如本书讨论过的，它可以使一个另类币更易实现自我增长的循环发展，通过增加总算力从而提高其抗攻击能力。这种情况下，想通过购买算力去破坏另类币的恶意竞争对手就需要付出巨大的前期投资。

另一方面，有人可能会认为这是一个安全假象。因为恶意竞争对手可以通过共同挖矿来产生比特币，收回一部分前期投资，同时，使攻击另类币的边际成本变得很小。把恶意竞争者看成规模很大的比特币矿工，也许更易于理解。事实上，前文提到的夭折的盘旋币，就是允许共同挖矿的。攻击者矿池Eligius和参与攻击者并不需要停止比特币挖矿就可以展开攻击。事实上，矿池的参与者甚至都不知道他们的计算资源被用于攻击另类币。



另类币的挖矿谜题趋势

截至2015年，无论是否允许共同挖矿，很少有另类币使用和比特币一样的SHA-256开采难题。这表明，SHA-256算法被认为是有安全隐患的。Scrypt算法^[1]是更受欢迎的选择，因为它使得比特币的ASIC在挖矿或者攻击另类币上变得毫无用处。不过，用于莱特币挖矿所制造的Scrypt ASIC矿机可用于攻击它们。

站在一个理性矿工的角度，当我们思考是否会共同挖矿时，我们会发现共同挖矿有很多安全问题。本书之前曾简略地谈到，只有当期望收益大于期望成本时，挖矿才有意义。对于比特币挖矿来说，成本主要是计算哈希值。但是对比特币矿工来说，决定是否和另类币共同挖矿并不会对哈希计算成本产生影响。额外的成本来自其他方面：计算、带宽、用于验证另类币交易的存储空间，以及需要使软件实时更新及在另类币出现硬分叉或者软分叉时，做出非正式决定。

这样的推理引出两个有洞察力的观点。第一，共同挖矿有很强的规模效应，因为所有的矿工所花费的成本相同，不管其哈希算力有多大。这与比特币有明显差异，因为在比特币体系中，成本和哈希算力成正比。对于小的低价值另类币，由于低的哈希算力，一个小的独立矿工公开挖矿的成本超过了回报，因此其无法获利。截至2015年，通过挖另类币获得的收入只占了比特币收入的很小一部分。这预示着，与比特币体系比，共同挖矿的另类币将会更具中心化。

有预测指出，大部分矿工会选择外包来对他们的交易进行验证。另类币规模越小，矿工就越有动力去找外包。最简单的办法就是加入比特币矿池。因为矿池通常替代矿工进行运算。矿池管理员验证比特币和另

类币区块交易，收集添加包含另类币的比特币区块。矿工只需专注于解决挖矿谜题并找出需要的数值。这个预测与实际非常贴近。比如，G池（GHash.IO），曾经最大的比特币挖矿池，同时允许对域名币、IX币（IXCoin）和Dev币（DevCoin）共同挖矿。这些也同时成为最受欢迎的共同挖矿另类币。

第二个观点，从经济学的角度讲，也许更加让人担心安全性而不是挖矿能力太集中。如果矿工的主要成本是工作量证明，在这种模式设计下，矿工是无法作弊的。在哈希函数的安全性保障下，挖矿没有捷径，并且其他矿工很容易并且也愿意去验证工作量证明。但是如果主要成本变成交易验证时，以上两个假设就不成立了。矿工倾向于假设他们收到的交易都是有效的，并不对这个交易做任何其他验证。而且，矿工如果要去验证一个区块及其交易，其工作量就和挖矿一样。因此，可以预期对于小的共同矿工，他们有动机跳过验证环节。由于存在不验证的矿工，攻击变得更加容易，因为一个恶意的矿工可以创建一个区块，让其他矿工对哪条是最长的有效区块链产生争议。

简而言之，共同挖矿在解决一个安全问题的同时，却也产生其他多个问题，部分原因是共同挖矿和单独挖矿在经济收益上有重大差别。总体来说，考虑到挖矿攻击，共同挖矿对一个新的另类币是否是一个好主意还很难说清。

[\[1\]](#) Scrypt是由著名的FreeBSD黑客Colin Percival为他的备份服务Tarsnap开发的。Scrypt不仅计算所需时间长，而且占用的内存也多，使得并行计算多个摘要异常困难，因此利用rainbow table进行暴力攻击更加困难。scrypt没有在生产环境中大规模应用，并且缺乏仔细的审察和广泛的函数库支持。——译者注

10.5 不可分割的交叉链互换

在比特币体系里，在不同个体或群体之间，达成一项交换货币或资产的交易很直接。这就是第6章里谈到的合币的原理。合币也可以用来交易智能资产，第9章简要提到，第11章会再进一步讨论。本章前面谈到的在域名币中出售域名也是基于同样的原理。

但是前面所有的例子中，即便涉及不同的资产，交易也都是限制在单一的区块链里。一般来说，一个另类币的交易和另外的其他另类币的交易历史没有任何关系也无法相互参考，这是一个基本的无法跨越的限制。那么，是否有其他办法可以互换不同的货币？比如，如果爱丽丝想卖掉 a 个另类币给鲍勃，换得鲍勃的 b 个比特币，他们可以把这项交易做成是单一且无法分割的形式吗？初看起来好像不太可能，因为无法强迫不同体系的区块链同时发生相关的交易。如果其中一个人，假设是爱丽丝，先执行交易，有什么办法可以阻止鲍勃不遵守承诺呢？

有个聪明的办法可以做到，这用到了密码学的承诺和锁定时间存储，这是两个我们已经讨论过的技术。图10.6描绘了这个协议。暂时先假设两个区块链里的区块是按固定步骤轮流产生的，每个时间单位产生一个区块。 T 代表协议流程的开始时间。

- 1 爱丽丝创建如下 a 个另类币的可以退还存款：
 - 1.1 爱丽丝创建一个随机的字符串 x，计算哈希值 $h = H(x)$
 - 1.2 爱丽丝创建如下图所示存储 A 区块，但是并不公开
 - 1.3 爱丽丝创建再融资 A 区块，让鲍勃签名
 - 1.4 一旦鲍勃在再融资 A 区块签名，爱丽丝公开存储 A 区块（但是还没有公开再融资 A 区块）
- 2 鲍勃创建如下可以退还的存款 b 比特币：
 - 2.1 鲍勃创建如下图所示存储 B 区块，但是并不公开
 - 2.2 鲍勃创建再融资 B 区块，让爱丽丝签名
 - 2.3 一旦爱丽丝在再融资 B 区块签名，鲍勃公开存储 B 区块（但是还没有公开再融资 B 区块）
- 3 情景 1：爱丽丝按照计划完成兑换
 - 3.1 在 T_1 爱丽丝索回比特币，把 x 给鲍勃（和其他所有人）
 - 3.2 在 T_2 索回另类币
- 情景 2：爱丽丝改变主意，不要比特币^①，也不让鲍勃知道 x 值
 - 3.1 在 T_1 鲍勃索回他的比特币
 - 3.2 在 T_2 爱丽丝索回她的另类币

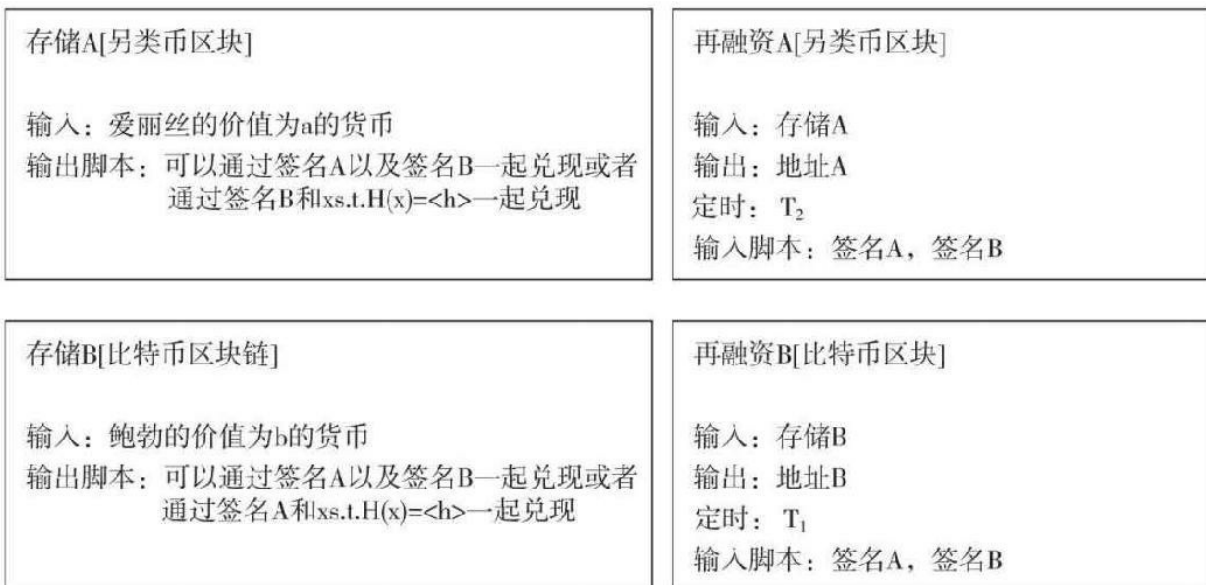


图10.6 不可分割的交叉链互换协议

①原作者写的是另类币，应该是笔误。——译者注

第一步，爱丽丝存储a价值的另类币〔这里的存意味着把货币发给输出脚本（ScriptPubkey），并在里面注明只有两种情况可以使用这笔货币〕。这个存款只有通过以下两种方法可以取得此a价值另类币：第

一，如果爱丽丝和鲍勃两个人都同意，他们可以取回。事实上，爱丽丝只有在鲍勃签署回款交易后，她才公开这个存款。这样就保证如果两个时间单位过去后，存款还没有被领取，她可以赎回她的存款。

另外一个办法是在任何时候，提供鲍勃的签名和 x 的值，通过 x 的值去开启哈希函数的承诺 h 。注意，把 $\langle h \rangle$ 写在存储A的区块里来表明爱丽丝特意把 h 写入输出脚本。因为只有爱丽丝知道 x ，所以在最后阶段，任何单独一方无法索取存款。这个方法就是，当且仅当爱丽丝拿到比特币，鲍勃才知道 x 的地址，他才能索取另类币。

第二步大体是第一步的反向过程。鲍勃存 b 单位比特币，这些比特币只能在两种情况下才能被取走。很重要的区别是，鲍勃并不需要创建一个新的谜题。相反，他用相同的哈希值 h （把这个 h 值从存储A区块简单复制到存储B区块）。哈希值 h 就是链接两个区块链的钥匙。

这时，爱丽丝有主动权，她可以临时变卦。如果在 T_1 时，爱丽丝还没有表示要给鲍勃 x 值，鲍勃可以简单地取回他的存款退出交易。爱丽丝的另一选择是在 T_1 之前取走鲍勃的比特币，但是她必须创建并广播输入脚本，里面含有 x 值。鲍勃看到这个广播就可以用 x 值去领取爱丽丝的另类币，兑换的交易完成。

注意，如果爱丽丝稍微晚点领取鲍勃的比特币（在 T_1 之后但是在 T_2 之前），鲍勃可能同时拿走两笔存款。类似地，如果爱丽丝及时拿走鲍勃的比特币，但是鲍勃等太久还没取走爱丽丝的，那么爱丽丝也可以把两个都拿走。但这不是问题，只要保证双方无法在协议上欺骗对方就可以，自己的疏忽或者故意怠慢不是系统考虑的范围。

最后，区块在比特币和另类币中，并不是按照固定时间产生的。这种情况会造成一些混乱，特别是两个区块链没有协调一致时。假设两个区块链各自平均10分钟产生一个区块。以1小时为时间单位，也就是说，需要 T_1 至少为现在另类币区块+12， T_2 至少为现在比特币区块+6，

也许能带来更大安全边际。

遗憾的是，存在很小的可能性，12个另类币区块已经找到，但后面6个比特币还没有找到。这时，爱丽丝可以索取两个存款。可以通过增加时间单位来降低可能性，但是会牺牲速度。

这是一个清晰明了的协议，但是截至2015年，还没有人用到。相反，所有加密货币都是在传统的中心化的交易系统里交易。造成这种现象有很多原因：第一是该协议的复杂、不便和缓慢；第二，这个协议可以防止偷盗货币，但是不能防范服务性攻击。有人或许以诱人的兑换价格作为广告，但是在协议原型的第一步或第二步就反悔退出，这浪费了每个人的时间。为了减缓这种情况，也为了集合并匹配大家的需求，可能需要一个中心化的交易平台（机制），即使如此，也不能完全相信它不会偷你的货币。这种情况进一步降低了该协议原型的使用范围。

10.6 侧链——基于比特币的另类币

本章前面部分探讨过给现有比特币所有者配置新的另类币的两种方法：或者要求用户把比特币销毁从而得到另类币，或者简单地把另类币发给现有比特币所有者，这些所有者必须拥有还没有用掉的比特币。正如我们看到的，任何一种方式都不需要另类币的价格盯住比特币。没有这种汇率锁定机制，在发展初期，另类币的价格会变化很大。**侧链**

（sidechains）的目的就是避免另类币价格变化太大，因为价格的波动太大会导致很多问题，也会使另类币分心乏术，无法真正专注于技术上的竞争。

下面介绍使另类币的价格以固定汇率的形式盯住比特币的相关技术。首先，所有者必须把所拥有的一定数量的比特币放入托管账户，这样才能创造出一个单位的另类币（或者固定单位的另类币），这样所有者才可以在另类币区块链上正常使用另类币。最后，所有者必须能够销毁自己拥有的另类币，从而取回之前存在托管账户上的比特币。这种构建像零币，通过托管基础币而创造零币。区别在于，需要在两个不同的区块链里进行上述操作。

遗憾的是，据我们了解，由于比特币的交易无法被其他区块链的事件所影响，目前还未找到可以不改动比特币而达到这种效果的方法。截至目前，比特币的脚本还没有强大到可以确认整个单独的区块链。好消息是，我们可以通过相对实用一点的软分叉来修改比特币，这也是侧链的原理。侧链的愿景是，将比特币作为储备货币，打造多种蓬勃发展、快速创新和实验的另类币。截至2015年，侧链还只是一个提案。但是比特币社区正在积极参与这个提案，目前已取得一些实质性的进展。侧链的提案还处于变化之中，所以为了便于学习和理解，我们适当简化了一些细节。

扩展比特币的功能，使之能够使侧链兑换成比特币，最显而易见但不太实用的办法是：把所有侧链的规则，包括验证所有侧链的交易和检查侧链的工作量证明，都包含在比特币体系里。这个方法不实用是因为这样会使比特币扩展出来的程序过于复杂，验证比特币的节点会非常困难。而且，链接上的侧链越多，复杂度和困难度就越大。

SPV技巧

可以使用SPV证明技巧来避免这种复杂局面。在第3章中，我们曾提到简单付款验证（Simple Payment Verification，简称SPV）。SPV可用于小的客户端，比如手机上的比特币应用程序（APP）。SPV节点不需要对其不感兴趣的交易做验证，它们只校验区块的标题。SPV客户只看他们感兴趣的交易，并确信是在最长的区块链内，并不担心该链是否是最长的有效链。因为他们假定矿工在创建该区块链并花精力去挖矿之前，已经验证过里面的交易了。

也许，可以扩展比特币的脚本让它能验证侧链里某些特殊的交易（比如销毁一个侧链币的交易）。在比特币里使用这种延展命令的节点，仍然会全面验证比特币的区块链，但是在侧链里，可能只会验证相对轻量级的SPV。

对一个交易提出异议

这种方法要好一些，但仍不完美。即使做最简化的验证，比特币的节点仍然要链接到侧链的点对点网络（每个链接上比特币的侧链都需要如此），并且追踪所有侧链区块的标题用于决定侧链最长的分支。最终我们想要的是：当一个交易要把侧链的货币转化成为比特币时，它本身就包含比特币节点需要的用于验证其合法性的所有信息，也就是说，验

证特定的侧链是真实发生的。这就是SPV证明的定义。

这里介绍一种可行的办法，唯一的缺憾是这个侧链的组成部分还在进一步研究中。为了在比特币里可以对照到侧链，用户必须证明：

（1）侧链区块里包含侧链交易；（2）侧链的标题表明这个区块已经接受过一定次数的认证，这意味着一定数目的工作量证明。比特币会验证这些证明，但是不会去验证这个区块头部展示的链是最长的。相反，比特币会等一定的时间，比如1~2天，让其他用户去找证据证明，第二步所指向的区块标题并不在最长分支上。一旦在特定时间范围内出现这样的证据，比特币体系中，接受该侧链交易的区块将会被认定为无效。

隐含的逻辑是：如果一个SPV证明已经可以确定，该交易不在最长分支上致使其不应该被认可，那么应该有一些侧链的用户会因认可这个交易而遭受损失。这些可能遭受损失的用户，有动力去辩驳SPV证明。如果没有用户遭受损失（也许是有一个分支，或者重组侧链，而且该交易也恰好在别的分支上），那接受这个证明也无妨。

一般来说，系统这样设计，对侧链问题并非毫无漏洞，系统也不会阻止你自己搬石头砸自己的脚。如果你把比特币转成有加密隐患的侧链，其他人也许能偷走你的侧链币然后再转成比特币。或者，在侧链的挖矿，也许会因为侧链漏洞而全部崩溃，导致对应的比特币也被偷。但是可以肯定的是，侧链的问题不会毁掉比特币；具体地说，不管侧链有多少漏洞，所有者都无法在侧链上兑现两次同一货币，也就是说侧链不允许比特币挖矿。

通过权益证明精简SPV证明的案例

还有一个障碍需要跨越。有些侧链生成区块的速度很快，也许每几秒钟就能产生一个区块。这种情况下，对比特币节点来说，单单验证

SPV证明就已经负担很重了。这时，可以用一个比较聪明的统计学方法，大幅减少对N个区块的验证，也就是大幅减少 $O(N)$ 的认证次数。

原理如下：当验证深藏在区块链中的一个区块，其实是在验证每个建立在这个区块上的所有的区块都符合**目标困难度**（target difficulty），即满足哈希值<目标值。这些区块的哈希值均匀地分布在（0，目标值）的区域，从统计学角度看，这意味着大约25%的区块可以满足哈希值<目标值/4。事实上，寻找N/4个区块满足哈希值<目标值/4的工作量和计算N个区块满足哈希值<目标值的工作量一样。这个数字4并无特别，我们可以用任何数代替。

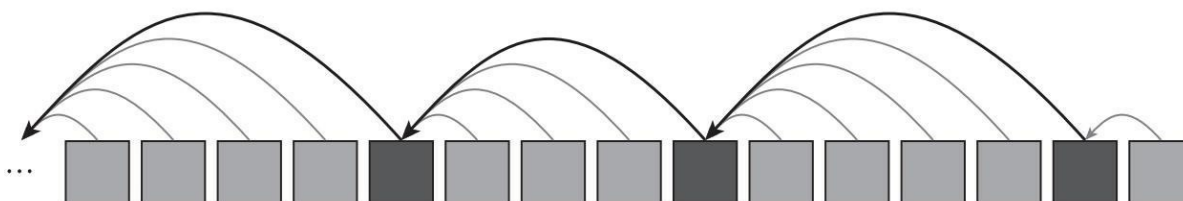


图10.7 工作证明跳表（proof-of-work skip list）^[1]

注：区块包含指向前面一个区块的指针和指向最近的满足哈希值<目标/4的指针。这个原理可以重复运用，比如一个第三层级的指针指向满足哈希值<目标值/16^[2]

这就意味着如果找到某种方法可以知道哪些区块满足哈希值<目标值/4，仅验证这些区块（或者区块的头部）就可以使用1/4的工作量完成全部任务。如何找到哪些区块满足哈希值<目标值/4呢？其实答案在区块本身。图10.7显示，每个区块包含指向前面一个区块的指针，以及指向最近的满足哈希值<目标/4的指针。

可以压低目标值到多小？是否可以选择很大的数，让目标值变得非常小？答案是否定的。这种方式的原理就像矿池，却是反方向的操作。在矿池里，矿池管理员验证大家的份额，也就是验证这些难度系数低（比较高的目标值）的区块。矿工找到比区块更多的份额，所以矿池管理员必须多做一道验证程序的工作。这样做的好处就是，能够比较精准

地估计矿工的哈希算力——估计值的方差较小。

我们来看相反的交易。随着估算建造整个区块链的工作的减少，估算值就有很大的方差。例如，假设 $N=4$ ，在没有使用跳表的方案下，会检测到有4个区块满足哈希值 $<$ 目标值。如果一个恶意的竞争对手要欺骗我们，他需要花4倍于我们找到一个区块的平均工作量才能办到。

假设这个竞争对手只做了一半的工作。可以算出，竞争对手有14%的机会能找到4个区块满足哈希值 $<$ 目标值。相反，在跳表方案下用4作为倍数，竞争对手的任务变成需要找到一个区块，满足哈希值 $<$ 目标值/4。在这种情况下，懒惰的只做了一半工作的竞争对手，却有40%的机会骗过我们，而不仅仅是14%。

[1] 跳表是一种随机化的数据结构，目前开源软件Redis和LevelDB都有用到它。——译者注

[2] 16是2的1+3次方。——译者注，以此类推。

10.7 以太坊和智能合约

我们已经介绍了几种用比特币的脚本语言写出有趣的应用的方法，如有托管功能的支付交易。我们也看到比特币脚本语言的一些瓶颈：只有很少的指令，并不符合图灵计算的标准。因此，很多新的另类币增添与应用程序相关的特殊功能。域名币是第一个尝试，后来又有许多加密货币，类似于比特币但是支持赌博、股票发行、市场预测等。

设想我们不需要为了每个应用程序，每次都建设一套新的系统，而是创造出一个加密货币系统，以支持所有未来可以想象到的任何应用。这就是所谓的图灵完备——据我们理解，满足图灵完备标准的编程语言，可以让你写出图灵机可以完成的任意功能，它可计算的函数和图灵机可计算的函数是完全相同的。因此，每一图灵完备的编程语言——包括我们熟悉的Java、Python和Lisp——都是图灵等价的。如果不考虑实际中的简单性和表现，图灵完备是我们在编程语言有关表达能力上需要的最好的性质。

从某种程度上讲，今天加密货币的发展使人回想起20世纪40年代早期计算机发展的时代：在第二次世界大战时，建造大量的复杂的只有某种特定功能的计算器（比如用于暴力破解密码的机器和海军用于确定发射弹道轨道的机器），这些工作促使研究专家致力于建造第一个可重复编程的通用计算机。任何可预见的应用程序都可以使用该计算机（见图10.8）。

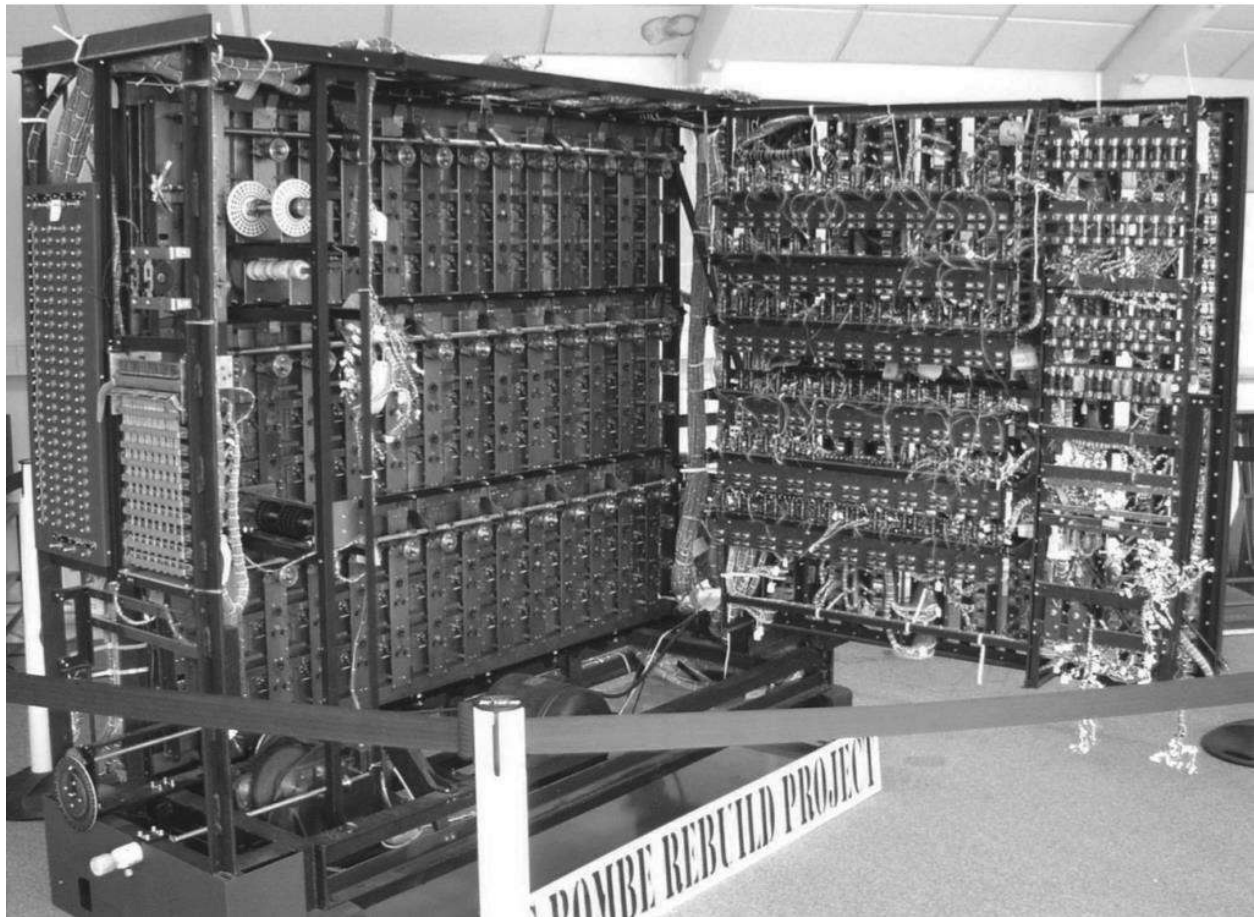


图10.8 在布莱切利园 (Bletchley Park) 博物馆重建的炸弹机 (Bombe)

注：炸弹机是一个由阿兰·图灵 (Alan Turing) 设计的特殊功能的高级计算机，用于破解德国的英格玛 (Enigma) 密码。通用计算机取代类似炸弹机的精巧装备，比特币能否也能像这样取代特殊功能的另类币呢？

以太坊 (Ethereum) 是一种雄心勃勃的另类币，致力于提供一种满足图灵计算要求的可编程语言，用这种语言可以编写脚本或者合约。虽然有其他方案可以做到这一点，但是以太坊无疑是最引人注目的：它使用了几个创新的技术，成功地完成了众筹，在几个月内筹资两千万美元，并且采用激进的参数，比如使用较短的产生区块的时间参数。以太坊系统本身很复杂，需要再编写一本新的教材才能完整阐述，本节只做简要讨论。

智能合约编程模式

智能合约最初是用来指使用计算机系统（或者其他自动化方式）来执行合约。例如，你可以把自动售货机看成一个销售商品的智能合约，执行的就是你和机器主人之间关于如何购买一个糖果的合约。

在以太坊体系，一个合约就是一个存在区块链里的程序。任何人支付一点费用，就可以用特定的操作将他的程序上传，建立一个以太坊合约。这个合约是用字节码(bytecode)写的，可以被特殊的以太坊专用虚拟机（Ethereum-specific Virtual Machine，简称EVM）执行。一旦合约上传，便永远存在在区块链里。智能合约有它自己的资金账户，其他用户可以调用程序里面开放的应用程序编程接口(API)，合约可以收发款项。

一个简单的例子：以太坊中的域名币

我们说以太坊可以用来执行任何特定应用的另类币功能。举个简单的例子，我们可以展示使用一个简单的以太坊合约，来构建出域名币形式的功能。

图10.9 所示就是一个构建的案例。它是以“稳健”语言（Solidity）编写，“稳健”是以太坊里用于定义合约的高级编程语言。这个合约产生一个原始的域名/数值（name/value）储存配对或者注册名。名字永远连着数字。这个合约定义了一个数字变量——注册表（registryTable），里面有32比特长字节和公开密钥的配对关系。初始时期，每个字节都对应着空地址0x0000000...000。这个合约同时定义了单一入口点，叫“用户名称”（claimName）。这个入口点只接受名字参数。首先，这个合约确认调用这个合约的人已经支付了至少10个wei。wei是在以太坊里最小的货币单位。如果没有支付10wei，合约自动终止并发出错误信号（“throw”的编程命令就做这些）。如果足够的wei已经发出而且这个名字还没有被注册，那么这个名字就和调用的地址永久地联系在一起。

```

contract NameRegistry {
    mapping(bytes32 => address) public registryTable;
    function claimName(bytes32 name) {
        if (msg.value < 10) {
            throw;
        }
        if (registryTable[name] == 0) {
            registryTable[name] = msg.sender;
        }
    }
}

```

图10.9 一个用于实现域名注册功能的简单以太坊智能合约

以上就是这个8行代码的合约能做的事。我们还可以多花点时间，把其他域名币有的功能都在这个合约里实现。比如，可以存储拥有者地址以外的信息，通过存储上次更新时间来要求域名的主人定期地重新注册，并且允许其他用户拥有长期不更新的域名权。

我们还可以加第二个功能，允许钱回撤。按照初始的代码设计，钱只能不断堆积在合约里，也就意味着从流通中消失。当然，在可以回撤钱的程序里，最好能设定，调用回撤的是合约的主人。任何人在以太坊都可以调用任何方程，但是用户是指定的，所以能确认谁是真正调用方程的人。

燃料、激励和安全

和比特币不一样的是，以太坊支持循环语句，虽然第一个例子里并不需要循环。循环语句一听就容易让人产生警觉，因为有循环的地方就会有无限死循环。从根本上说，以太坊合约有可能因为种种原因而无限循环。计算机领域里一个著名的研究结果（难以判断的终止问题）证

明，不存在任何算法，可以根据源代码去判断一个程序是否可以无限运行下去。因此，我们如何防止合约无限运行下去呢？

更进一步讲，即使条约不会无限运行，也需要某种方式来限制它不会运行太久。以太坊体系通过一种称作“燃料费用”的机制来实现这一点。简单地说，每执行一条虚拟机器的指令需要花费一小部分的成本费用，我们称之为“燃料费用”。不同的操作花费不同。基本的像加减操作只花费1单位燃料费用，而计算SHA-3哈希值（内置函数）需要20单位燃料费用，在永久存储器上写256比特长的字符需要100单位燃料费用。每笔交易也需要先支付21 000单位燃料费用。你可以把以太坊体系想象成超级折扣的航空公司。机票只是你支付乘飞机的费用，任何其他需求都要多付钱。完整操作清单和固定的燃料费用都可以从以太坊里找到。任何清单和费用的变动都需要以太坊产生一个硬分叉，这和比特币脚本语言的语义改变一样。

燃料费用是通过以太坊体系内部被称为以太（ether）的货币来支付的。它只是在用来支付合约操作的时候才叫燃料费用。每笔交易都规定了燃料的价格，也就是说，每份燃料需要多少以太。燃料费用就像比特币的交易费，矿工可以自由公布交易的燃料费用，每个矿工都可以独立地决定收费方式。这样会得出一个反映市场供求关系的燃料市场价格。2016年年初，虽然以太坊网络体系还是属于实验阶段，市场已经默认50 gigawei为1单位价格。50gigawei等于 5×10^{-8} 以太，根据以太币和比特币2016年1月的汇兑比例，这也就是大约 3×10^{-10} 比特币。

每次调用之前，必须设定燃料费用的最高限，也就是愿意支付价格的最大值。当达到这个值（燃料用完了），程序就会终止，发生的所有程序状态的变化就会被重新设置到原始状态，但是矿工还是保留燃料。由此可见，不要用完燃料，这一点非常重要。

燃料的使用要求，意味着以太坊不适合很耗费资源的计算。以太坊

系统未被设计成像云计算那样的服务，即支付一定的费用让云服务完成自己无法做到的计算。像亚马逊的弹性计算云或者微软云计算平台，提供划算百万倍的计算量。另一方面，以太坊更加适合创建安全逻辑协议。本质上来说，以太坊提供了一种两个或者多个匿名交易者可以信赖的服务系统。

以太坊上区块链的安全还没有像比特币一样完善。理论上，以太坊比较复杂，也比较难以用数学推理来论证。实际上，以太坊才刚刚开始发展，其安全性还没有像比特币一样经过很多考验。尤其是，担心处理交易的成本会让类似比特币的激励机制失效，我们在共同挖矿的分析中讨论过存在这种担心的情况。当交易成本占矿工的总成本的比重不再能忽略不计的时候，大的矿工有明显优势，因为成本和哈希算力相互独立。更重要的是，燃料只支付给最初包括该交易的区块的挖工。但是所有的在这之上建立区块的矿工都必须验证该区块，却得不到任何报酬。这意味着，他们将有动力去跳过该验证。正如之前所看到的，这种情况不利于区块链体系的健康发展。

第二个例子：以太坊体系中的国际象棋

我们还没涉及以太坊中新功能如何运用，所以让我们看第二个案例。假设爱丽丝和鲍勃下国际象棋，赌注是一定数额的金钱。唯一的问题是爱丽丝和鲍勃生活在不同的国家，他们都不相信对方输了会支付赌注。这个问题可以用以太坊来解决。

爱丽丝写下以太坊程序，这个程序设定了国际象棋的规则并且被上传到以太坊网络。她给这个合约支付一定数量的以太作为赌注。鲍勃可以看到这个合约，如果他答应接受挑战，他把他的赌注支付给这个合约，就等于开始了这个游戏。鲍勃在接受挑战之前应该确认，这个合约是准确无误地遵守了国际象棋的规则，并且最后会把所有赌注支付给获

胜者。

一旦双方都支付了赌注，假设他们约定下同样的赌注，合约会检查双方的赌注是否相等。这时候，游戏就开始了。任何一方除非赢了游戏，否则无法从合约里取出钱来。其他人在任何情况下也无法取得这笔钱。

爱丽丝和鲍勃轮流把自己的下棋步骤发给这个合约。这个合约也会检查轮到谁下确保指令是由爱丽丝或者鲍勃发出，而不是其他人。大家是否还记得调用者需要在每个操作（促使合约执行一个动作）上签名，因为合约可以根据签名确认调用者。合约也会根据国际象棋的规则校验双方的步骤。如果一方试图把兵移动3格，合约会拒绝该步骤。

到最后游戏结束。合约在每一步都会检测是否有一方被将军，或者双方打平，或者满足其他打平的条件。玩家也可以发送投降的指令。当游戏结束时，合约终止，并把所有的钱支付给获胜者，或者平局下平分赌注。

从概念上看，这是一个以太坊的简单应用，但是有很多微妙的地方值得探讨。如果一方快输了他就放弃了？合约应该设定一个机制，如果一方在规定的时间没有提交有效的下一步，钱就支付给另一方。

哪个玩家先走呢？白方先走的话，白方就拥有微小的优势。因此，双方都想做白方。这就碰到了以太坊合约的一个难题：没有内置的随机源。之所以是一个难题，是因为随机数发生器需要所有矿工的检验（因为他们需要检验合约是否正确地执行），但是这些随机数对任何人来说都是不可预测的（否则的话，玩家也许就因为不能先走而拒绝参加这个游戏）。

随机数“信号塔”(randomness beacons)可以解决这个问题。正如9.4节讨论的，在双方都加入游戏后，合约计算区块链下一个区块的哈希值。

对这个特定的游戏应用而言，这个问题比较容易解决，因为只要让爱丽丝和鲍勃双方确信决定谁先谁后是随机的，这样就满足要求，而不需要向所有人证明。所以他们可以采用9.3节的办法：他们两个同时提交一个随机数的哈希值，并且公开他们的输入值，然后从双方的输入总值算出随机数。实际操作中，以上两种方法都可以使用。

其他应用

下棋也许很有趣，但是真正激动人心的是以太坊在金融领域的应用。我们在课本里讨论的大部分应用，包括市场预计、智能资产、托管支付、微支付渠道和混合服务，都可以在以太坊体系里实现。这些应用都有其细微的区别，但是相对比特币死板的协议，大多数情况下，这些应用都能相对容易地在以太坊体系内完成。

以太坊的状态和账户余额。 第3章中，我们讨论了账本两种方法：基于账户和基于交易。在一个基于交易的账本中，如比特币，区块链只存储交易（加上一些少量的转载标题的设置数据）。为了方便验证交易，比特币的币值是无法分割的，即交易的结果必须整体被消费，可以自己消费，或者如果需要的话，换地址消费。交易实际上是在全球状态表上操作的，这个表称为“未花费交易输出列表”。但是比特币的协议并没有明确规定这个全球状态表。全球状态表的产生纯粹是矿工为了加快验证过程而创造出来的。

另一方面，以太坊则是基于账户的模式。由于以太坊已经存储了合约地址和状态的对照表的数据结构，很自然地也同时存储每个普通地址（或者叫拥有者的地址）的账户余额。这意味着，与非闭环式的交易支付模式必须有输入和输出不同，以太坊存储每个地址的账户余额，这一点，与银行存储每个账户余额的方式类似。

以太坊的数据结构。 在第3章，我们提到基于账户的账本需要精心设计的数据结构来存储记录。以太坊就有这样的数据结构。具体来说，每个区块包含每个地址的目前状态（账户余额和交易数）的摘要，同时也包含每个合约的状态（余额和存储空间）。每个合约的存储树结构映射256比特的地址和256比特的字节。这样可以存储巨量的

$(2^{256} \times 256 = 2^{264})$ 信息。当然，这只不过是理论上的可能空间，我们不会用到这么大的存储空间。数据结构里面提供的摘要，使验证一个地址有多少余额或者空间变得相对容易。比如，不需要鲍勃从头到尾扫描整个区块链，爱丽丝就可以向鲍勃证明她有多少余额。

此时，比特币用简单的二项梅克尔树的结构可以派得上用场。因为它可以把有效的证明数据存在该区块里（要求矿工确信对于相同的地址，每个树状数据结构都要求该地址相同的状态）。但是我们也希望能够更快地查询地址并且能够有效更新地址的数值。为了达到这个目的，以太坊使用比较复杂的树状结构，叫帕特里夏树（Patricia tree）、前缀树（prefix tree）、字典树（trie）或基数树（radix tree）。每个以太坊区块包含梅克尔-帕特里夏树（Merkle Patricia tree）的树根，它保存每个地址的状态，也包含合约地址。每个合约的状态，包含一个树状数据结构用来保存合约的存储状态。

基于账户账本的另一个不易处理的问题是防止重复攻击。在比特币里，每个交易都使用“未花费交易输出列表”输入，因此，任何相同签名认证过的交易，不可能被重复使用两次。但是在以太坊设计里，需要确保当爱丽丝签下支付给鲍勃1以太交易的时候，鲍勃不能一次又一次地对外广播并重复使用这个1以太，直到把爱丽丝的账户用光。这样的交易不能重复，因为一旦使用了，爱丽丝的交易计数会增加一次，而这个交易计数是一个全局的状态参数。

总的来说，以太坊使用比比特币更加强大的数据结构来管理它的账本。虽然我们没有深入研究它的数据结构，但我们知道，这个数据结构

使得账户、合约，以及交易相关声明的有效验证变成可能。

以太坊项目

以太坊最早于2013年年末开始讨论，并于2015年第一次发布，代号先行者（Frontier）。以太坊采用预售的方式，以固定比特币价格公开出售，并把所有的预售款投入以太坊基金会。

和其他另类币相比，以太坊发展比较缓慢，这也反映了以太币是一个比较复杂的系统。与比特币相比，以太坊增加以太坊专用虚拟机（EVM），一个全新编程模式，一个全新的数据结构。此外，以太坊还对比特币的共识模式做了大的修改。每个区块产生的时间不是10分钟，而是12秒。在以太坊体系里，过时区块的比例高于比特币体系，为了减少过时的区块对系统的影响，以太坊采用另一个叫“精灵”（GHOST）的协议来计算共识分支。同时，以太坊采用不同的工作量证明。目前采用的是一个混合的哈希方程，被设计成只能用记忆体计算。未来以太坊计划转为通过权益证明份额证明的体系。

以太坊呈现出和比特币在设计理念上的巨大差异。以太坊项目由非营利机构主导并且在规划和决策上相对比较集中，它们根据历史经验对以太坊协议进行修改，并且都有一个公开的时间表。按规划，将来也会有硬分叉。而且，所有以太坊合约都要在版本更新前销毁。所以，以太坊还是一个未来会有很多变更的实验性体系。截至2015年，投入大量精力在以太坊上并构建真正有用的应用，现在看来是有点太早。但是以太坊无疑是一个非常有潜力的系统。也许这本书未来的版本将会命名为“以太坊和加密货币技术”。

本章主要讨论了比特币如何成为其他加密货币和另类币的重要组成部分。它们在各方面相互竞争、合作并且相互影响，有些相辅相成，有

些是相互阻碍。在未来，可能会出现新的技术，使得在一种区块链可以直接引用另一个区块链的交易。

但截至目前，有些问题仍然悬而未决。另类币会演变并相互合并，最后成为少数另类币主宰的生态系统吗？还是和现在一样多样化？特定功能的另类币会蓬勃发展，还是以以太坊为标志的通用编程平台最后成为主流？比特币和另类币之间的相互影响是有益的吗？每个另类币之间应该相互独立，比如用不同的挖矿谜题而不是去共同挖矿？我们现在无法回答上述这些问题，但我们已经讨论了所有这些你需要理解和评估的重要概念。

延伸阅读

侧链白皮书：

Back,Adam,Matt Corallo,Luke Dashjr,Mark Friedenbach,Gregory Maxwell,Andrew Miller, Andrew Poelstra,Jorge Timón,and Pieter Wuille.“Enabling Blockchain Innovations with Pegged Sidechains.”2014.

您可以通过如下网址阅读：

<https://blockstream.com/sidechains.pdf>.

关于域名币和使用其他用加密币设计域名/价值储存方法的论文：

Kalodner,Harry,Miles Carlsten,Paul Ellenbogen,Joseph Bonneau,and Arvind Narayanan.“An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design. Presented at the Workshop on the Economics of Information Security,2015.

您可以通过如下网址阅读：

<http://randomwalker.info/publications/namespaces.pdf>.

以太坊白皮书:

Various authors.“A Next-Generation Smart Contract and Decentralized Application Platform.”

您可以通过以下网址阅读:

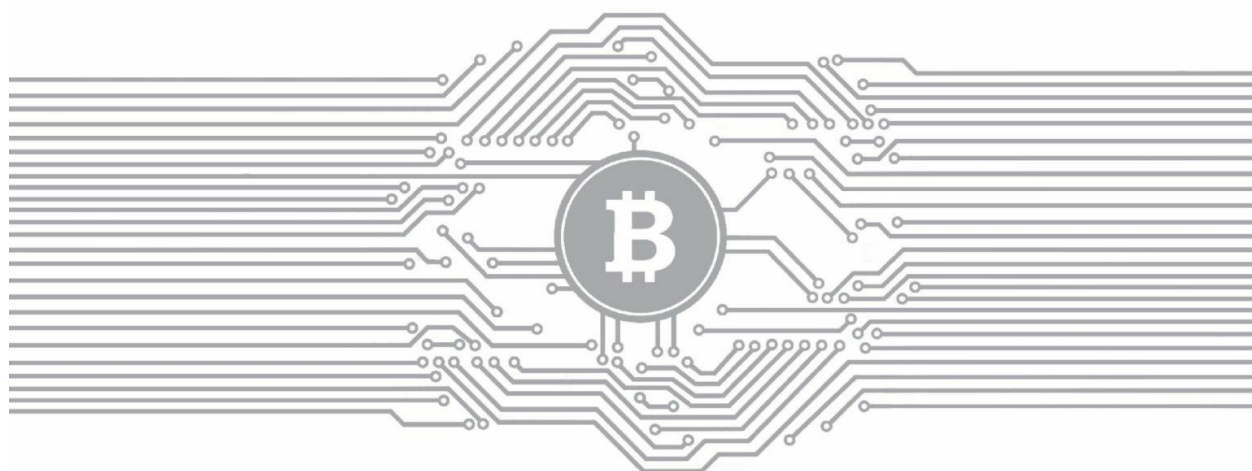
<http://github.com/ethereum/wiki/wiki/white-paper>.

分析以太坊激励机制错配的学术论文:

Luu,Loi,Jason Teutsch,Raghav Kulkarni,and Prateek Saxena.“Demystifying Incentives in the Consensus Computer.” Proceeding of the 22nd ACM SIGSAC Conference on Computer and Communications Security ,New York:ACM, 2015.

第11章

去中心化机构：比特币的未来？



这本书写到这里，我们已经研究了比特币和区块链技术截至2015年的最新状态。本章将讨论的是，比特币在未来会怎么样。我们恪守箴言“绝不预言，特别是预言未来”，所以我们不会声称知道比特币未来会怎么样。因而我们在本章标题使用了问号。

但是我们继续本书中一直坚持的学术探讨风格，用以研究未来的科技。比特币的未来充满了热情和叹为观止的未来科技革命的前景。本章可以写成一个宣言，但我们不准备这么做。我们找出知名的方案，用谨慎冷静的方法对它们分类，并批判地分析它们的相对优势和劣势。

比特币是一个内容丰富的课题，它包含了协议本身及其成为新应用平台的潜在可能性。本章的重点不在于比特币协议的未来。虽然我们意识到有很多影响比特币未来且值得研究的方面，比如，比特币的管理、效率、扩展性和功能集合。

我们会着重讨论比特币如何成功地成为去中心化的货币，它的成功经验能促使我们重新思考其他中心化的机构——比如从事股票、债券、资产产权和其他业务的机构。我们不禁会问，区块链是否能够用来对它们去中心化。我们不仅仅要考虑技术上去中心化的可能性，还要考虑，它是否合乎金融规律并对社会有利？

11.1 区块链作为去中心化的工具

在比特币之前，有很多数字电子货币失败的尝试（本书的前言中提到了许多失败的案例）。比特币与大多数失败的尝试之间，最重要的区别在于去中心化。比特币去中心化的核心创新方法是使用区块链。

在这一节，我们会研究区块链技术如何在货币体系以外的领域里实现去中心化。本章我们会一直重复使用汽车的案例，这辆车的所有权是通过区块链来控制的。这个案例是我们在第9章中介绍的智能合约的概念里的具体体现。早在1990年年初，尼克·萨博（Nick Szabo）和其他几位创新性提出智能资产和管理智能资产的数字化合约，远远早于比特币。随着区块链的出现，这个想法变得越来越现实和具体。

令人鼓舞的案例

当代的汽车使用两种主要的加锁机制（locking mechanisms）：门上的物理锁和通过电子锁住引擎不让发动的制动器。用户用遥控钥匙可以与汽车无线通信，根据遥控器与车的距离或者用户按下按钮的特定动作，来解锁车门和发动引擎。

为了防止假冒钥匙入侵，车钥匙的解锁机制需要加密。虽然安全专家发现很多最近使用的加锁机制存在很多问题，但是他们是有可能处理好这些问题的。一般来说，这些算法会使用对称钥匙加密技术。在这个案例中，用的是基于非对称加密技术的类似椭圆曲线数字签名算法的数字签名技术。

在这个例子里，汽车储存了一份遥控器的公开密钥，用于打开车门

和发动引擎。当遥控器请求开门的时候，汽车发送回随机数并要求遥控器用它储存的密钥签名。只有遥控器准确回复签名，车门才会被打开。到目前为止，这个原理和实际中的防盗机制没有什么大的区别。唯一的区别是，我们使用了很深的加密技术，安装起来比较昂贵。

实现智能

这次设计的智能汽车，是假设用来验证遥控器的公开密钥并不是靠汽车制造商永久地记录在汽车里；而是，智能汽车技术上可以不间断地，无线接收例如比特币一样的区块链上的新区块。当汽车在组装厂组装的时候，遥控器里第一个用户（比如组装厂的经理）的公开密钥通过特殊操作加入区块链。同时，这辆智能汽车也把该特殊操作的ID写入它自带的程序。

核心的思想是，汽车更改所有权的时候——从装配车厂到质量监控室到运输人员到汽车经销商到第一个所有者——也同时更新到区块链，区块链同时授权每一步的转换。值得注意的是，在这个模式下，授权用的遥控器没有跟着车走。每个人或者公司都有一个预先存在的遥控器（或者带着某种有遥控器功能的仪器）。这个遥控器里面有一个唯一的签名密钥。根据区块链的交易，签名密钥被激活或者被取消拥有这辆车的权利。这样的交易以车最新的交易ID为输入，同时设定一个新的公共密钥为输出ID。汽车目前的拥有者需要用私人密钥在这个输出ID上签名。

这种设计和我们在第9章讨论的智能资产相似，除了一个重大的区别：区块链的交易不仅仅表示汽车所有权的变更，它还代表真正的汽车物理拥有权的转移。当汽车通过区块链转移的时候，前车主的遥控器无法工作，新车主的遥控器获得开门和启动引擎的权利。让所有权等同于使用权的技术有着深远的影响，这将促使强有力的去中心化。但是去中

心化是否有用，这并不容易看清楚。我们将在11.4节回过头来讨论这个问题。

安全的交易

假设爱丽丝拥有一辆智能汽车想卖给鲍勃，能够数字化地转移汽车控制权会引起几个有趣的可能性。比如，爱丽丝也许正在国外旅行正需要钱来支付旅费，所以要卖掉停在她家后院车库的汽车。只要联上互联网，鲍勃就可以用比特币支付给爱丽丝车钱，爱丽丝可以远程通过区块链把车的所有权转移给鲍勃，鲍勃就可以开走这辆车。

然而，这样的交易存在一定的风险。如果鲍勃先支付，爱丽丝也许收了钱而不转移车的所有权。如果爱丽丝先转移车的所有权，鲍勃也许不付钱就把车开走了。即使假设爱丽丝在现场，也有可能另一方突然改变主意而撤销交易。这时候让不在场的第三方来调解争议也很困难。

我们之前多次碰到这种问题，包括在合币（第6章）和域名币（第10章）中。解决这类问题要使用同样的原则。只要支付的货币和汽车的拥有权同时存在相同的区块链，爱丽丝和鲍勃就可以产生一个不可分割的交易。这个交易同时转移汽车的所有权和车款。具体地说，这个交易规定两个输入：爱丽丝的所有权和鲍勃的支付款；规定两个输出：归鲍勃的所有权和归爱丽丝的支付款。这个交易需要双方提供输入要素，因此要求双方都要签名。如果只有一方签名，交易就无效。一旦一方签名，交易的细节就无法改变，除非这个签名无效。签过名的交易一旦对整个区块链广播，鲍勃只要等预设的几次确认(一般是6次)，就可以拥有这辆车。鲍勃支付给爱丽丝的款项也同时被确认。两个确认是相辅相成，缺一不可的。

细心的读者也许注意到了一个问题。鲍勃可以收到爱丽丝签

名的交易，自己也签名，但是不立即对外广播。等到爱丽丝卖东西的价格变了，鲍勃才把旧交易用原来的价格对外广播。所以为了避免这种问题，比较复杂的不可分割的交易里包括截止时间。过了截止时间后，爱丽丝可以发送输入她控制下的新地址，用来表示撤回她发给鲍勃的已经签过名的交易。

这是本章案例之一。我们将会在本章看到，很多其他案例使用区块链技术促使现实中的各种交易程序去中心化，从而达到不同种类的去中心化状态。其中，不可分割性（atomicity）是绝大多数案例共有的特性。也就是说，交易每一方的交割都是联系在一起的，所以它们都同时发生或者都不发生。不可分割性是区块链以外应用程序领域里重要的安全概念。

11.2 通往区块链融合之路

因为比特币的区块链是专用在货币上的，把它改造为用于表示其他应用是很有挑战性的。在比特币世界里，你会发现有许多人偏爱把比特币或者别的区块链作为去中心化的平台。在本节，我们来分析两种方法。

方法1：直接在比特币基础上

区块链融合自然而然的出发点是比特币。这也是我们在前面11.1节智能汽车例子里用的办法。直接使用比特币的好处就是容易实现——代码容易运行，比特币网络有很强的挖矿能力，共识过程没有瑕疵。然而，我们必须在比特币上做些修改才能用于我们的例子。比如，用于授权比特币交易的加密要等同于用于打开车门的加密。有时候对比特币的修改是不可能的，而且从根本上说，如果你有非常复杂的涉及不同方的合约，用比特币的区块链不一定能足够胜任或者不可分割地执行。为了展示用比特币区块链的危险性，我们研究一下如何构建一些中性的非中介化的应用程序。

首先，我们来研究众筹服务。在2015年，最广泛使用的众筹网站是Kickstarter，它通过一个中心化的网站，连接了创业者和资金提供方。我们欣赏Kickstarter的想法，但希望通过建造一个完全去中心化的替代系统。这个系统需要让创业者能要求投资人捐款，但是在收到一定预先设定数额之前，创业者不能花掉任何一分钱。所有的这些都是没有中介的。

用比特币的技术实现这样的众筹服务，需要创业者创建一个特定输

入的交易（输入数可以随着进程而改变）和一个支付给自己的输出，比如支付1 000个比特币（BTC）。这个交易将在潜在的资助者中流传。任何资助者都可以把资助额加在交易的输入上，并且数字化签名他们的输入和总输出。只有到所有输入等于或者大于输出的时候，创业者才能取得这笔交易的所有输入（见图11.1）。因为签名形式有限，我们要用到比特币一些鲜为人知的功能，才能花掉最后的交易额。虽然这在当今的比特币系统能做到，但是我们必须钻研到比特币里很少人知道的角落。这并不是一个日常见到的标准比特币交易。

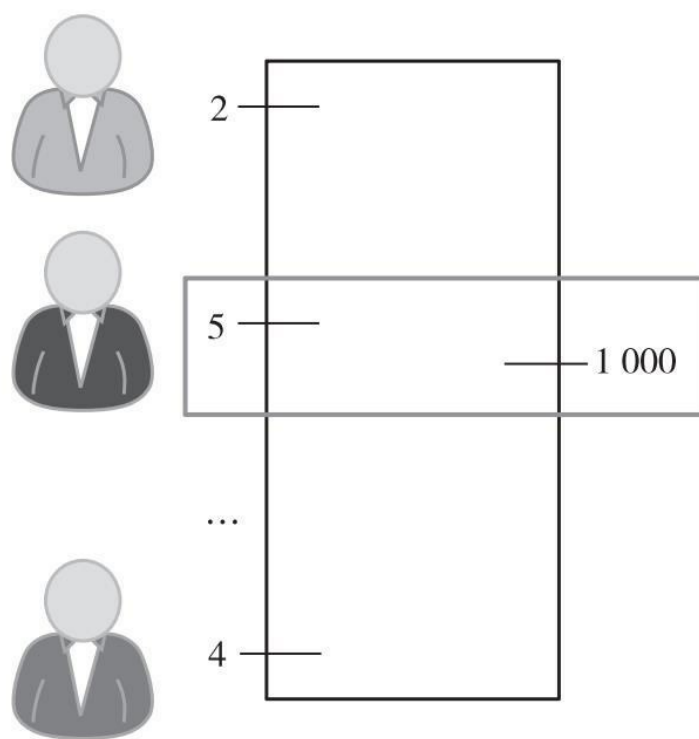


图11.1 通过比特币众筹

注：由不同资助者发起的多输入的单笔交易。每个资助者签下他们的输入和输出。只有在累积输入数额达到或者超过输出，该交易才有效。

另一个案例：**支付证明费用**（paying for a proof）。这个案例初看起来好像奇怪，但是它有很重要的应用。为了表示清楚，我们假设有个哈希函数 H 和一个大家都知道的数字 y ， y 是 H 输入 x 后产生的输出。爱丽丝知道这个 x 的数值，鲍勃为了知道这个 x 值，愿意支付给爱丽丝。广

义上讲， H 可以是任何计算程序，鲍勃希望知道他感兴趣的能够产生特定结果的输入值。这个问题的进一步演变是，鲍勃也许愿意支付一定的费用，让这个输入值公开在区块链上。

为了安全地实现这笔交易，我们必须确认交易的不可分割性。爱丽丝只有提交正确的输入才能收到钱。而鲍勃一收到输入必须承担支付责任。记得我们在第10章的不可分割的交叉链互换协议中，展示了如何绑定支付和呈现哈希函数输入值。类似的方法可以用在这里。

这些例子显示了直接使用比特币区块链的重要局限性。在每个例子中，我们必须把复杂的真实世界交易编译成比特币的概念。这不一定总能实现。在智能汽车的例子里，我们假设该车用ECDSA签名技术来验证汽车的主人。这就允许我们使用区块链和遥控器相同的公/私密钥来开锁并发动汽车。在众筹例子中，创业者只能拿到他们要求的数额，不能多也不能少。如果资助的金额大于需求的，多出的部分就成为交易费用。最后，在支付证明费用的例子里，如果函数 H 不是比特币语言所支持的哈希函数，那么连接支付和公开数字这种模式就很困难。

如果你不能，或者不想把应用程序强行套入比特币的交易体系，那么可以选择使用附着币，我们在第9章讨论过附着币。这样比特币就成为数据存储，因此比特币的脚本语言如何表达就与之无关。这种用附着币的方式，不仅可以构建很多其他应用，还可以使应用透明化。重新回到卖车的例子，如果区块链中对象的颜色是公开的（比如以有颜色的货币来表示），任何人都可以通过检查区块链得知汽车在何时购买，以什么价格，而不用知道买卖双方的真实身份。这种方式在某种情况下很有用。在对它不利的时候，颜色的对象可以不对外公开。

然而，这种附着币有重大缺陷。附着币的用户无法依靠比特币的矿工来验证交易（因为矿工无法了解附着币的交易语言含义）。这意味着所有附着币的用户必须以全网节点的方式运行。SPV也不可能。只要在构建的时候存在使得共识无法达成的漏洞，附着币就会变得很不稳定。

如果两个附着币对一个交易的有效性持不同意见，会导致这个货币形成两个分叉货币。这会导致灾难性的后果。相反，如果由矿工来验证交易，这种不同意见的情况就会很少发生。如果这种情况真的发生了，那么它很快就会引起注意并且很可能解决，而不会导致货币分叉。

从另一方面考虑，无论我们是否用附着币，用比特币的初始范畴外的交易会加重或者“污染”比特币的区块链。在比特币世界，这个问题双方争执不下。我们不选边站，但是我们要指出有一个解决的办法：就像我们在9.1节看到的，仅仅把比特币当成时间戳服务，而不是当成数据存储。目前有刚刚起步的服务，提供另外的区块链或者数据存储服务。其中有一个服务是通过比特币区块链做时间戳服务。这就像第9章讨论过的时间戳服务，但是多了每10分钟一次哈希计算，而不是每周一次在新闻报纸上。用比特币当时间戳只要每区块（或者每次服务或者协议）一次交易。不完美的地方就是，很难找到像比特币区块链这样容易获得并且广泛复制留存的外部数据存储。同时，一般的非比特币数据存储更加中心化。

总的来说，不管是否使用嵌套技术，比特币的区块链诞生了许多创新的应用。这些通过比特币区块链产生的应用，受到用户和矿工的广泛接受。因此，使用比特币区块链是一个安全且容易实现的选择。

方法2：另类区块链

去中心化的另一个方法是使用另类区块链，也有几个选择方案。最明显的方法就是，使用一个全新的区块链，有自己的规则、功能和货币（也就是另类币）。另一个方案是，使用我们在第10章学过的侧链。这个方案的主要不同在于侧链的货币是1：1的比例方式与比特币挂钩。有高级脚本语言的侧链可以满足复杂合约的要求，也能做到去中介化。但是，侧链需要对比特币进行修改，这些修改目前到2015年还没有进展。

第三个选择是用已经存在的另类区块链，这个区块链能够支持新的应用程序。截至2015年，我们在第10章讨论过的以太坊体系，是最有潜力的去中心化加密货币应用程序平台。从概念上看，以太坊是去中心化的复杂合约的理想平台。当然，以太坊也面临实际的挑战：至少到2015年，它还没有达到比特币同等水平的成熟度、接受度和挖矿计算力，也没有接受相应水平的安全性考验。无论如何，这是一个令人着迷的去中心化复杂合约的精美实验。未来，以太坊体系或者其他体系有可能蓬勃发展。

11.3 去中心化的模板

我们研究了几种通过区块链达到去中心化的方式。接下来，我们将建立一套去中心化应该考虑的问题的模板，问题包括去中心化的对象、用什么区块链合适、实体和安全性在去中心化下的重新定义。

去中心化的程度

通过去中介而去中心化

再回想一下我们前文提到的智能汽车，为了帮助理解，我们问一个问题，数字拥有权的转移到底替代了现实生活中的什么步骤？

美国汽车的产权，是由拥有产权证书来确定的。这是产权的中心化形式。产权证书只有机动车管理部门（Department of Motor Vehicles，简称DMV）能识别和实际使用。当出售汽车的时候，卖方交接产权证书给买方，仅仅这样做是不够的。这样的产权转移，必须在DMV注册，DMV在其中央数据库进行更新。通过区块链来转移产权，我们从国家掌控的集中程序转变成不需要任何中介。这就是通过去中介来实现去中心化。

争议的调解：通过竞争去中心化

假设买卖双方对汽车交易有争议。也许卖家出售了一辆以次充好的汽车，买家很生气要退货。在第3章，我们讨论过3选2的多方签名交易。如果除了买卖双方以外还有第三方比如法官或者调停者，这个交易就可以支持托管。这种情况下，买方不需要直接把钱转给卖方，而是转

到一个由买卖双方和调停者组成的3选2控制的地址。调停者在另外一方的帮助下可以批准支付或者退款，但是不能偷走这笔钱。

这是一个很好的争端解决机制的开端，但仍有很多细节需要考虑。首先，我们丧失了以前依赖的汽车交易的不可分割性。其次，我们不清楚汽车的拥有权是否可以随着退款而恢复原来的状态。最后，如果汽车的所有权转到3选2的地址，那么遥控钥匙要给谁开车的权利？我们讨论这些的目的不是找出解决这些问题的办法，而是用这个例子来仔细思考调停者的作用。具体而言，我们要比较这种调停模式和传统调停模式的区别。

现实世界里的调停争议如何发生？这需要借助司法体系，一个中心化的、国家控制的，最好需要聘请律师的调停系统。相反，在数字合约下，参与者自由选择他们想要的调停者。一个调停的私人市场将会蓬勃发展。在这个市场里，不需要按现有的法律规定，各种潜在的中介可以根据公平、效率和成本相互竞争。这中间有几个挑战性的问题：第一个是激励机制，调停者也许会被交易的一方贿赂；第二个是资金在有争议期间是被锁住的；第三，当内部调停机制失效后，因为交易双方都是匿名的，所以很难最后上法庭解决，即使双方可以被识别，数字合约当前也不被法庭认可。

我们的观点是，这不是通过去中介而产生去中心化——我们没有完全摆脱中介，而是让参与者选择他们信任的人。也就是说，通过竞争去中心化。在介于单一规定的中介和完全不需要中介的完全去中介之间，还有很大的空间和可能。就像我们看到的，在这两种极端之间，可以存在一种情况，即有很多中介相互竞争。事实上，我们在第9章讨论去中心化的未来预测市场也是这种情况。不像InTrade^[1]一个公司占领整个市场，参与者可以从竞争的仲裁人中任意选择他们相信的人来进行关键的市场操作。

能达到什么样的安全程度

我们从这个案例观察到另外一个问题。诊断解决过程的安全性不需要依靠不可分割性。相反，它依靠对调停者的信任。调停者如何变得可信？有很多种办法，最直接的就是通过信誉。与不可分割性通过技术维持安全性不同，信誉是建立在长时间的社会内部机制相互作用的基础上的。



信任

有人在比特币世界里把“信任最小化”或者“没有信任”作为目标。这听起来像是退步。难道我们不是希望建立一个值得信任的可以运作的体系？

信任这个词有不同的解释，因而会引起不同的误解。当爱丽丝借给鲍勃10美元并说信任他，爱丽丝的意思是她觉得鲍勃是个信得过的人，她坚信鲍勃会还钱。在安全术语里，一个可信任的组成部分意味着你不得不依靠的对象。当人们用可信任来描述认证机构的时候，他们觉得如果这些机构都不可信了，网络安全就毫无保障了。

在其他条件都不变的情形下，信任最小化是一个值得追求的目标。我们希望能打造一个安全的系统，这个系统能够尽量减少我们不得不依靠的组成部分。但是当你手里有把铁锤，任何事情看起来都像可以用铁锤来解决的钉子。比特币的支持者经常过度追求去除体系中的可信任部分。一个可信的组成部分不总是坏事。现实世界里存在的信任关系本身也没有问题。去除可信任的部分，可能带来其他隐藏的问题。

我们在本章最后的11.4节会详细阐述这一点。至少到目前为

止，我们意识到信任这个词的复杂含义，我们避免信任这个词，而是用安全这个比较明确的词来表示。

在技术解决不了的地方，或者作为技术解决方案的补充，信誉起了一定的作用。然而，信誉也有一些问题。信誉是要和真实身份联系在一起的。如果真实身份不确定或不明朗，信誉就无法发挥作用。比如，一家餐馆收到网络差评后决定关了该餐馆，摆脱坏信誉，然后以原班人马重开一家新的餐馆。在匿名的世界，信誉无法发挥作用。在半匿名环境下，真实身份很容易改变，以信誉为基础的系统会面临很大的挑战。信誉体系也要设法去验证对别人声誉有影响的众多评价。在传统的像 Yelp^[2] 的系统中，商户用真名，用户某种程度上也用真名。然而在半匿名环境，很难精确地区分是假的指控还是真的事实。

我们不再深入讨论其他的安全机制，比如安全硬件设备等。不管是用什么安全机制，最后都会面临一个大的挑战，即没有现实生活中的执法机构。因为没有用真实身份，这些机制里都没有对错误行为的惩罚，争议也无法在法庭上解决。借钱变得不可能，因为没有执法机构保证借款人会还钱，因此交易经常需要先预存款，这些预存款在争议期间会被锁住。

框架

总结一下本章至今讨论的内容，我们可以通过提4个问题，来对任何去中心化的方案进行分析：

1. 去中心化的对象是什么？
2. 去中心化的程度如何？

3.用什么样的区块链？

4.采用什么样的安全措施？

只要回答了以上4个问题，我们就基本上能精确地了解大多数在比特币世界里见过的基于区块链的去中心化方案。让我考虑以下几个例子（见表11.1）：

智能资产

我们讨论过的智能资产，去中心化的是资产的所有权和资产的转移。它达到了完全去中介化——完全不需要DMV和国家这样的实体。我们谈过它如何使用比特币的区块链来达到目的。当然你也可以用另类区块链。最后，安全性是通过不可分割方式，即把支付与汽车所有权的转移不可分割地融合在一起。

表11.1 区块链去中心化的方案特征

特征	方案			
	智能资产	去中心化的 预测市场	存储 J	零币
1. 去中心化的对象是什么？	资产所有权和转移	预测市场	文件的存储和调用	混合币种
2. 去中心化的程度如何？	去中介化	竞争和去中介	竞争	去中介
3. 用什么样的区块链？	比特币	另类币	比特币	另类币
4. 采用什么样的安全措施？	不可分割	声誉，不可分割	声誉	不可分割

去中心化的预测市场

在一个中心化的预测市场，中心平台或者交易所提供两种重要的服务：裁决并公布任何赌注的事件，并向参与者出售股权（或者帮助参与者安全地彼此交易）。我们在第9章看到，去中心化的预测市场不需要一个中央权力机构来提供这些功能。它让每个人都可以为一个时间设置一个市场，并通过发送一个简单交易，成为对应市场的仲裁者，这样降低了执行这些操作的准入门槛。因此，中介还是存在的，但用户可以自由选择很多相互竞争的中介。如果用户还不满意，他们自己可以来执行这些操作。另一方面，用户可以直接自动地和其他用户交易股票，所以中央集权这方面的功能被去中介化了。去中心化的预测市场要求比特币没有的新功能，所以最好通过一个定制的另类币的区块链来实现。

存储J

存储J(StroJ)是格雷戈·麦斯威尔（Greg Maxwell）提出的，用于文件存储和调用。它已经有好多更新版本，但我们只讨论简单版本。大体上看，存储J设置了一个存在云端的“代理”，它被设计过，能自己做出一些特定决定。比如，为了有计算资源，它可以租用云端算力和存储空间。另一个提供给用户的功能是让客户将文件存放一段时间，比如24小时，需要用比特币付费。只要收到比特币支付，它就会一直保存客户文件。除了简单的存储，它还能做一些其他有趣的事情。我们不做深入展开。在我们的框架里，存储J实现了文件存取的去中心化，这也是像Dropbox^[3]一样中心化服务的核心功能。代理其实就是中介。对我们来说，自动化与否其实并没有区别。然而，中介之间存在竞争。支付是通过比特币。代理提供服务和收到支付并没有不可分割的连接，所以安全是通过代理的声誉来实现的。

零币

我们在第6章讨论过零币，一个有效的、去中心化达到混合币种从而保持匿名服务的方法。零币不是采用中心化的混合服务，而是采用加

密协议实现了用混合币种的功能，只是靠数学和共识而不靠中介。零币和它的后来者重度使用加密机制，因此比较适合使用特别的区块链。在安全措施上，我们曾提到需要销毁一个基础币（Basecoin）从而作为交换获取一个零币，这两个操作密不可分。赎回零币也是如此，这就是典型的不可分割性。

[1] 一个在线电子交易平台，对应的在线赌博模式被称为“未来事件交易”。网站用户可以对所有与体育竞赛没有关系的“大事件”下注，包括政治事件、经济形势、娱乐新闻、交通运输、法律现状、流行音乐甚至是天气情况。——译者注

[2] Yelp类似于国内的大众点评。——译者注

[3] 一款非常好用的免费网络文件同步工具，是Dropbox公司运行的在线存储服务，有人说是世界上最伟大的云存储服务之一。通过云计算实现互联网上的文件同步，用户可以存储并共享文件和文件夹。——译者注

11.4 什么时候适合去中心化

我们一直在关注技术上如何实现去中心化。现在，我们要深入研究去中心化的动机。这些问题跟技术无关，却同样难以回答：去中心化一定是有益的吗？经济上合适吗？去中心化的社会影响是什么？

我们至今只是把“去中心化”当成一个技术概念，却从来没有明确提出去中心化是和政治紧密相关。当我们讨论用技术的创新手段替代或者部分替代传统体系，我们实际上是在讨论如何在旧有的法律、社会和金融机构中重新分配权力。去中心化的理想来自比特币的起源：密码朋克运动——一群不墨守成规的人发起的旨在通过加密技术实现个体自治的运动（参阅前言和第7章相关内容）。有了区块链，他们的理想相对以前更近了。但是他们的理想可行吗？受欢迎吗？

回到我们的汽车销售案例，传统机构会试图帮助汽车所有者解决两个问题：第一个是强化所有权，也就是说，防止偷窃；第二个是确保交易安全进行，或者说防止在交易中被欺骗。所以当我们比较智能资产和现有体系时，我们不能仅仅比较一切顺利的时候谁效率高，最重要的是我们要看事情不顺利的时候，最坏能坏到什么程度。

现实生活中的安全性挑战

防止任何形式的偷盗——比如汽车、艺术品、现金等——都是预防、发现和纠正错误。预防性安全机制在于阻止偷盗的发生，发现性安全机制在于发现盗窃便于将来采取纠正错误的措施，纠正错误就是索回盗窃的损失并惩罚盗窃者（惩罚也可以看成是预防盗窃发生的方式之一）。车锁和报警器是预防性安全措施，GPS跟踪器(比如LoJack)用于

帮助发现盗窃并有助于执法者找到被偷的车。其中的关键在于，阻止偷车涉及警察、保险、法庭等，车锁只是阻止偷车犯罪的一个小因素。如果你生活在没有法律保护的环境里，单纯的车锁并不能阻止盗窃的发生。这种情况下，锁在路边的车很快就会被偷走。

智能资产的模式极大地依靠预防措施。只有把所有权等同于使用权，我们才能实现去中心化。即拥有这辆车所有权就表示，你知道某区块链上的私人密钥。但是这种控制原理无法取代我们现在拼图式的机构合作。

假若我们仅用保密的私人密钥来表示拥有权，那么数字加密就变得很重要。但是因为人类是所有因素里最容易被突破的，数字加密的保密性就会变得很困难。加密系统的设计者几十年来一直在努力让非技术用户使用并管理私人密钥以防止偷盗或者丢失钥匙，但是毫无进展。如果去中心化只依靠私密密钥，非法软件或者钓鱼攻击就能偷走车。或者忘记密钥就能导致你的车变成一堆废铁。当然，以上问题都可以有其他的解决方式，最后这些解决方式让我们回到中介和中心化系统，偏离了我们为之奋斗的去中心化的主旨。

只要涉及人，资产转移就会存在争议如何解决的问题。争议在于交易条件或者交易的任何一个方面。在现实世界，如果交易双方无法达成一致，就会把争议提交到法庭，法官会按照固定的程序验证每一条证据、供词和书面文件，最后法官会做出关于这个买卖有效性的判决。很多人，特别是技术方面的人，倾向于把法律看成是一套由逻辑化的规则与算法组成的体系，该体系必定能够得到一个明确的裁决。然而，现实中的法律体系不但有冗长的法律和条约，还有人们对法律法规的理解和判断。这些离有明确逻辑的法规的观念就更加遥远了。这种特征并不是弱点。因为这样才可能允许我们去解决当初制定法律的人所没有想到的更加复杂的案例。

回到去中心化模式的安全问题，我们想要的安全属性和去中心化模

式提供的安全模式是有差别的。就以之前提到的去中心化众筹为案例：我们知道众筹可以技术上设置成让创业者直到资助款达到一定数额才可以取出。然而，这并不能阻止已经成功筹集到钱的创业者携款潜逃。事实上，即使在现在中心化模式下，众筹网站也有一些骗局，最终被告上法庭。在去中心化模式下，创业者有可能会匿名，没有被法律诉讼的威胁，这种情况下骗局一定更多。很难想象技术能够解决这个难题。这是另一个案例，显示了技术只能解决一小部分问题。坦白地说，技术能解决的只是问题中无趣的那部分。

小结一下，智能资产的问题是社会性的，都是当事情不太对劲时引起的纠纷。在所有参与方都满意的前提下，技术可以保证交易的高效性。但是，技术无法解决这些棘手的纠纷。

智能资产的优缺点

正如我们讨论的，在一些传统上需要人们介入的方面，智能资产不容易去中心化。事实上，自动化可能让去中心化更加困难，因为调停和其他进程都是在事件发生后才出现，自动化很难协调好这种事后出现的不正常的事件。最后，智能资产产权会产生新的问题，比如在汽车的例子中，会要求软件和硬件都安全。

在某种程度上，我们讨论过的例子只是一个完整智能资产协议的缩印简化版。比特币世界中的很多提案都是更为周全与细致入微的。即便如此，在我们简单的案例中，我们还是可以分辨出智能资产的好处和坏处。

智能资产的最大优点，就是能够在任何时候、任何地点进行高效的所有权转让。对于像智能手机或者电脑这样的产品，价值没有汽车那么高，如果有争议一般也不会诉诸法律，所以使用智能资产没有任何坏

处。对于这些产品，不可分割的交易是一种有用的安全性特性。

通过区块链的智能资产也可以提供很好的隐私保护甚至匿名服务。虽然我们说隐私保护会让解决争议变得复杂化，但对于一个消费者信息被公司滥用的社会，隐私保护还是很有意义的。在某些情况下，不需要揭露真实身份是交易方最看重的因素。这在中心化的中介模式下是不可能的。

最后，去中心化的模式允许自由选择调停者。即使我们对法律系统很满意，大多数争议调停是由像维萨或者贝宝这样的私人公司内部暗箱操作的。通过使用可替代的模式，让调停公开竞争，我们有可能让这个过程更加透明公开并接受公众的监督。

加密、国家和大机会

崛起的现代国家和我们在本章讨论的技术的目的有惊人的相似。在从氏族部落和小群体发展出来的现代社会，政府一直致力于精确地解决一个问题：让陌生人安心地开展商务和其他交互活动。政府和我们讨论的技术，采用的办法也许大不相同，但是目标是一致的。

尽管马克思主义者眼中的去中心化也许牵扯到解散国家，但解散国家这种做法不太现实，尤其是在其他人比如民主化国家的人民也希望去中心化时。然而，通过技术去中心化并不一定会和国家对立。事实上，它们可以相辅相成。比如，假设交易双方都是经过验证的，智能资产的交易就可以通过区块链技术高效地完成，万一有争议，也可以付诸法律。我们认为，未来区块链技术的机会就在于，以和政府功能互补的方式建立去中心化，而不是试图替代政府。

只要技术存在就可以去中心化，这种想法很吸引人。但是在实际操作中，我们需要找到经济上令人信服的理由，比如说政府的监管过于繁

杂和低效，或者权力失衡导致的权力滥用。举个例子，很多非洲国家的居民已经用“手机分钟”（cell phone minutes）作为实际上的货币，这样的货币脱离了政府的控制，也避免了相应权力的滥用。

总结一下，我们在本章描绘了去中心化的技术蓝图，也批判性地探讨了去中心化的动因。我们鼓励大家寻找去中心化更有说服力的案例，特别是把现有法律和监管实践融合在一起的好案例。

结束语

有些人因为其底层技术而对比特币感兴趣，另外一些人对它的商业可能性着迷，还有一些人关心它的社会和政治影响。理性的人可能不同意后面两类人的观点。但是我们希望这本书能够让你知道，比特币在技术上是具有深度的、创新的、有趣的，而且是建立在正确理论上的。我们才刚刚开始开拓比特币之外令人炫目的另类加密货币，其中的某些加密货币也许有一天甚至超越比特币。

我们选择深入研究比特币，是因为我们坚信技术的力量。我们坚信比特币和其他计算机科学有很深的联系。我们重点突出了有潜力的新技术是如何试图取代已有组织机构的。我们相信，人类还会继续找到加密货币技术在新的商业和社会领域里的有益应用。即使你的兴趣主要在于它的商业化，你也能从了解掌握它的底层技术中获益。而了解它的能量和限制，有助于你在市场的浪潮起伏中顺应时势。

未来何往？去中心化的好处之一，就在于它是一个极佳的实验和学习平台。任何人都可以下载安装和分析比特币的区块链，或者在此基础上建立自己的应用。我们希望你也能充分利用这些机会。

我们制作了许多教材的网络辅助材料。Coursera网上课程^[1]（www.coursera.org/course/bitcointech）包含了根据本书录制的视频课程，还有测验和一些编程作业（在线资料链接为<http://press.princeton.edu/titles/10908.html>）。参加这个网络课程还可以让你和志同道合的学习者一起在线讨论。

^[1] 免费大型公开在线课程项目，由美国斯坦福大学两名计算机科学教授（Andrew Ng和Daphne Koller）创办。旨在同世界顶尖大学合作，在线提供免费的网络公开课程。Coursera的首

批合作院校包括斯坦福大学、密歇根大学、普林斯顿大学、宾夕法尼亚大学等美国名校。——译者注

术语表

Advanced Encryption Standard 高级加密标准（简称AES）

altcoin infanticide 另类币夭折

Altcoin 另类币

anonymityset 匿名集

anonymous marketplace 匿名市场

Anti-Money Laundering 反洗钱（简称AML）

append-only ledger 仅增账目

Application Programming Interface 应用程序编程接口（简称API）

Application Specific Integrated Circuits 专用集成电路技术（简称ASIC）

Arithmetic Logic Units 算术逻辑单元（简称ALU）

ASIC-resistant puzzles 反ASIC解谜算法

asymmetric information 信息不对称

atomic cross-chain swaps 原子型交叉链互换

Basecoin 基础币

bent corner theory 折角论

Berkeley Open Infrastructure for Network Computing 伯克利开放式网络计算平台（简称BOINC）

birthday paradox 生日悖论

bit fiddling 数位操作

bitcoin core 比特币核心钱包

Bitcoin Foundation 比特币基金会

Bitcoin Improvement Proposal 比特币改进方案（简称BIP）

bitcoin mining 比特币挖矿

bitcoindlibrary 比特币官方客户端的资源库

bitcoin-qt library 比特币类库，现在又称为比特币中心（bitcoin core）

bitlicense 比特币牌照

block chain 区块链

blockchain.info 区块链信息公司

block-discarding attack 区块丢弃攻击

bootstrapping 自举过程

brain wallet 大脑钱包

bytecode 字节码

Byzantine Generals Problem 拜占庭将军问题

change address 零钱地址

chunk size 块大小

clustering of addresses 地址簇

CoiledCoin 盘旋币

coin center 货币中心

Coinbase 比特币基地公司

CoinJoin 合币

coinstake transaction 币拥有量交易

collision-resistance 碰撞阻力

collusion 串谋

Colored Coins 染色币

Commit Coin 承诺币

commitment 承诺

compatibility 兼容性

compression function 压缩函数

consensus chain 共识链

consensusalgorithm 共识算法

consolidating funds 资金合并

Counterparty 合约币

CreateCoins 造币

cryptocurrencyecosystem 加密货币生态系统

crypto-currency 加密数字货币

cryptographic beacons 密码学“信号塔”

cryptographic guarantees 加密学保证

Cunningham chain 坎宁安链

cypherpunk 密码朋克

Dark Coin 黑暗币

data furnace 数据火炉

deanonymized 暴露

decentralized mixing 分布式混币

default strategy 默认策略

digital cash 数字货币

digital signatures 数字签名

distributed consensus 分布式共识

distribution with high min-entropy 最小信息熵分布特性

Dogecoin 狗币

double spending 双重支付

ECDSA 椭圆曲线数字签名算法

efficient micro-payments 高效小额支付

encoding keys 编码解码

escrow transaction 第三方支付交易

Ethereum-specific Virtual Machine 以太坊专用虚拟机（简称EVM）

Ethereum 以太坊

feather forking 羽量级分叉

Field-Programmable Gate Array 现场可编程门阵列（简称FPGA）

Fischer-Lynch-Paterson impossibility result 不可能性结论

flooding algorithm 泛洪算法

flooding protocol 泛洪协议

forking attack 分叉攻击

frontrunning 预先交易

fully validating nodes 完全有效节点

fungibility 可互换性

Futurecoin 未来币

GenCoin 生成货币

genesis block 创世区块

getblocktemplate 获取有效区块模版（简称GBT）

GoofyCoin 高飞币

Great Internet Mersenne Prime Search 互联网梅森质数大搜索（简称GIMPS）

green addresses 绿色地址

Hash 哈希算法

hash collision 哈希碰撞

hash pointer 哈希指针

hash power 哈希算力

hash puzzles 哈希解谜

hash rate 哈希速度/哈希率

hashes of public keys 公钥哈希值

hiding 隐秘性

hierarchical deterministic wallet 分层确定性钱包

high min-entropy 高阶最小熵

high-level flows 高风险交易流

idioms of use 惯用法则

implicit consensus 隐性共识

instawallet 一种在线钱包

joint payments 共同支付

key stretching 密钥延展

key-value 键值

Know Your Customer 了解你的客户（简称KYC）

Large Hadron Collider 大型强子碰撞（简称LHC）

laundering hashes 洗算力

laundry 洗钱

lemons market 柠檬市场/次品市场

lightweight nodes 轻量节点

Linear Feedback Shift Registers 线性反馈移位寄存器(简称LFSR)

linking 关联性

Litecoin 莱特币

lock_time 锁定时间

locking mechanisms 加锁机制

mandatory reporting 强制上报

megajoules 兆焦耳，百万焦耳

megawatt 兆瓦，百万瓦特

memory-bound puzzles 内存限制解谜

memory-hard mining puzzle 记忆储存体挖矿谜题

memory-hard puzzles 刚性内存解谜

memoryless process 无记忆进程的

merge avoidance 合并规避

mergemining 共同挖矿

Merkle trees 梅克尔树

Merkle-Damgard transform MD 变换

mining shares 挖矿工分

Mix net 混币网络

Mixing 混币

modular addition 模加法运算

multisignatures 多重签名

Namecoin 域名币

niche currency 利基货币

nonce 临时随机数

opcode 操作码

Open Computing Language 开放运算语言（简称OpenCL）

open protocol 开放协议

OpenAseet 开放资产

open-source project 开源项目

open-source software 开源软件

open-source system 开源系统

orphan block 孤块

overlay currencies 附着币

parent node 父节点

partial hash-preimage puzzle 不完全哈希函数原像解谜

partial preimage 不完全原像

PayCoins 付币

paying for a proof 支付证明费用

pay-to-pubkey-hash 标准的比特币转账流程/支付到比特币地址的标准交易

Pay-to-script-hash 支付给脚本的哈希值（简称P2SH）

Peercoin 点点币

Permacoin 永久币

Petabytes 拍字节（简称PB）

Pigeonhole Principle 鸽巢原理

pool hopping 矿池跳换

Primecoin 质数币

private key 私钥

progress free 无关过程的

proof of burn 销毁证明

proof of Liabilities 负债证明

Proof of membership 隶属证明

Proof of non-membership 非隶属证明

proof of Reserve 准备金证明

proof of retrievability 可恢复性证明

proof of storage 存储量证明

proof of“clairvoyance” 未来预测证明

proof-of-stake 权益证明

proof-of-workskiplist 工作证明跳表

proof-of-work 工作量证明

protein folding 蛋白质折叠

provision 准备金

pseudocode 伪代码

pseudonymity 化名

Pseudo-Random Generator 伪随机数发生器（简称PRG）

publickey 公钥

pull requests 提交请求

Pump-and-dumpscams 拉高出货骗术

punitive forking 惩罚分叉

puzzle-friendliness 谜题友好

Quick Response code QR 码

race condition 竞态条件

radio telescope 射电望远镜

Random Access Memory 随机存取存储器（简称RAM）

randomness beacons 随机数“信号塔”

real scripts 实际脚本

reality keys 现实密钥

replace-by-fee 替代策略

reputation system 信誉评价系统

Request for Comments 评议请求（简称RFC）

root 树根节点

Satoshi bones 中本聪骨头

Satoshi Dice 中本聪之骰

Satoshi Nakamoto 中本聪

save up 蓄力

scriptPubKey 输出脚本

scriptSig 输入脚本

ScroogeCoin 财奴币

Secure Hash Algorithm 256 安全哈希算法（简称SHA-256）

secure timestamping 安全时间戳

selfish mining 自私挖矿

sidechains 侧链

sidechannels 旁路攻击

Simple Mail Transfer Protocol 简单邮件传输协议（简称SMTP）

Simple Payment Verification 简单付款验证（简称SPV）

smart contracts 智能合约

spare cycle 空闲周期

stack-based programming language 堆栈式编程语言

stake-grinding attacks 股权粉碎攻击

stratum 层

sybil attack 女巫攻击

taintanalysis 污点分析

tamper-resistant device 防损硬件

temporary block-withholding attacks 临时保留区块攻击

the 51 percent attack 51% 攻击

the head of list 链表头部

the nothing-at-stake problem 无利害关系问题

threshold cryptography 门限密码

threshold signature 门限签名

Tinkerbelle effect 仙子效应

transaction syntax 交易语法

transaction graph analysis 交易图谱分析

tumbler 翻洗

uniform transactions 一致性交易

uniqueCoinID 唯一的货币编号

unlinkability 无关联性

vanity addresses 虚荣地址

virtual currency 虚拟货币

virtual mining 虚拟挖矿

zero confirmation transaction 零验证交易

Zerocash 零钞

Zerocoin 零币

zero-knowledge proof 零知识验证

Zetacoin 泽塔币

译者简介

帅初，毕业于中国科学院，从2013年起，就从事加密货币和区块链技术领域的开发和研究工作，具备丰富的区块链行业经验。现担任唯链科技（vechain）首席技术官，也是中国区块链开源平台QtumChain的设计者。

蔡凯龙，点石资产管理创始人，厦门抬钱论道资产管理公司执委会主席，互联网金融千人会联合创始人，百度支付海外顾问，恒生电子海外投资高级顾问。注册金融分析师（CFA），金融风险管理师（FRM），经济和计算机双硕士，金融博士生。曾任联想控股旗下P2P翼龙贷副总裁，互联网金融千人会执行秘书长，德意志银行（美国）战略科技部副总裁，美国能源公司MXEnergy风控经理，美国休斯顿大学商学院金融系助理教授。《金融时报》（中文版）、《新浪财经》等财经媒体的专栏作者，曾发表多篇关于互联网金融的文章。编辑出版《智慧众筹：互联网金融早餐会》一书。

许余洁，现任联合信用评级有限公司研究总监，中国资产证券化研究院首席研究员，西南财经大学特聘研究员。2013年7月起供职于中国证监会研究中心（2015年更名为中证金融研究院），暨证监会博士后科研工作站与清华大学五道口金融学院联合培养博士后。2014年从事明斯基《稳定不稳定的经济》一书中文版的翻译校稿工作。近年来，在《人民日报》、《金融法苑》、《中国金融》、《工业技术经济》、《中国经济报告》、《中国证券报》等报刊杂志上发表文章30余篇，并以笔名“余吉力”在财新博客上坚持撰写100篇读书心得，广为转载。

李耀光，中国人民大学财政金融学院经济学硕士，特许金融分析

师（CFA），中国注册会计师（CPA）。现就职于某合资证券公司，担任结构融资总监，负责境内资产证券化、REITs及结构化金融产品的设计与发行，并参与跨境证券化产品与REITs的研究或顾问工作，成功完成或执行的资产类型覆盖商业及工业地产、应收账款、银行信贷、消费金融、租赁资产、公共事业收费权等。在此之前，曾就职于某行业领先的内资证券公司资产管理部、四大国有银行总行，长期从事理财与资金池投资管理、结构化投融资相关工作，并担任中国资产证券化研究院研究员，中国资产证券化论坛理事及教育委员会委员。

高晓婧，毕业于北京外国语大学英汉同声传译专业；曾就职于华夏银行总行理财业务管理部门，现就职于兴业银行总行投资银行部；具有多年泛资管领域从业经验，目前主要研究领域包括：银行理财、泛资管及资产证券化业务。

洪浩，CFA，现任职于中泰证券债券与结构金融部，负责信贷资产证券化和企业资产证券化业务。曾任职于中国对外经济贸易信托有限公司，在信托公司建立了全流程的服务体系。负责或参与十余单公募、私募资产证券化项目。北京大学理学博士，中国资产证券化研究院特聘研究员。

图书在版编目 (CIP) 数据

区块链：技术驱动金融/（美）纳拉亚南等著；林华等译. --北京：中信出版社，2016.8

书名原文：Bitcoin and Cryptocurrency

Technologies: a Comprehensive Introduction

ISBN 978-7-5086-6584-9

I. ①区... II. ①纳... ②林... III. ①电子货币—基本知识 IV. ①F830.46②TP3

中国版本图书馆CIP数据核字（2016）第182827号

区块链：技术驱动金融

著者：（美）阿尔文德·纳拉亚南 约什·贝努 爱德华·费尔顿 安德鲁·米勒 史蒂文·戈德费德

译者：林华 王勇 师初 蔡凯龙 许余洁 李耀光 高晓婧 洪浩

策划推广：中信出版社（China CITIC Press）

出版发行：中信出版集团股份有限公司

（北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029）

（CITIC Publishing Group）

电子书排版：张明霞

中信出版社官网：<http://www.citicpub.com/>

官方微博：<http://weibo.com/citicpub>

更多好书，尽在中信书院

中信书院：App下载地址<https://book.yunpub.cn/>（中信官方数字阅读平台）

微信号：中信书院

区块链

从数字货币到信用社会

长铗 韩锋 等◎著

BLOCKCHAIN

from Digital Currency to Credit Society



中信出版集团 · CHINA CITIC PRESS

区块链

——从数字货币到信用社会

长铗 韩锋 等 著

中信出版社

目录

序一 区块链：建设互联网的价值高速公路

序二 区块链：网络世界运行规则与技术的全新探索

序三 区块链——未来全球信用的基础协议

第一章 区块链创世纪

第二章 区块链基础

第三章 区块链进阶

第四章 智能合约

第五章 区块链怎么玩

第六章 从信息互联网到价值互联网

第七章 区块链政策与法规

第八章 区块链经济学的范式革命

后记

附录

序一

区块链：建设互联网的价值高速公路

姚余栋^[1]

区块链因比特币而生。一般民众都将比特币简单地视为一种货币，但从根本上来说，区块链更是价值传输协议。相较于通常意义上的数字货币，区块链与互联网TCP/IP（传输控制协议/网络互联协议）协议更为相似。只不过，TCP/IP协议为信息互联网而设计，区块链则为价值互联网提供了理论基础。

但在互联网上进行价值交换，需解决三个问题：一是确保价值交换的唯一性；二是如何确立价值交换双方的信任关系；三是如何确保双方的承诺能够完成依靠网络的自治机制（智能合约）而自动执行，而无需可信第三方的介入。2009年基于区块链技术的数字货币比特币的诞生，给上述三个问题找到了解决方案。

区块链是一种新型的去中心化协议，链上数据不可随意更改或伪造，因而提供了无需信任积累的信用建立范式。区块链可理解为一个账本（ledger），人们只需加入一个公开透明的数据库，通过点对点的记账、数据传输、认证或智能合约来达成信用共识，而不再借助任何中间方。这个公开透明的数据库包括了过去所有的交易记录、历史数据及其他相关信息。这些信息安全地分布式存储在一串使用密码学方法产生的数据块中，即为一个区块，从创始区块连接到当前区块，就形成了区块链。由于每个区块都包含了上一个区块的索引，即区块的哈希

（hash），使得每一个区块按照时间顺序产生，若要逆转某个区块上的交易，需要重新计算该区块之后的所有区块，这在计算难度上几乎是不

可能的。于是，区块链逐步成为一种可靠的审计工具，也让系统内参与者之间的信任建立得以实现。

区块链本身具有分布式（Distributed）、去中介（Disintermediation）、去信任（Trustless）、不可篡改（Immutable）、可编程（Programmable）等特征。这些特征使区块链能弥补传统金融机构的不足，提高运作效率，降低运营成本，灵活更新市场规则，防止信息篡改和伪造，同时也大大提高了稳定性，减少了宕机风险。因而区块链可应用的场景非常广泛，众多金融机构正在研究区块链技术在金融市场的应用。

区块链可直接用于银行相关业务。例如，对账户的反洗钱检查、交易后的银行结算等涉及人工审核的业务。区块链的分布式网络结构使账户资产、信用等信息可在各银行间共通，这大大简化了重复性手续，节省大量人力物力。目前，全球中央银行和商业银行都在积极寻求利用区块链技术，开发数字货币平台。R3CEV区块链项目在世界上获得多家银行支持，目前有42家银行加入该项目的研究，实现实时结算和清算功能。

各国央行还可以使用区块链技术尝试发行eSDR，来构建一套新型的超主权货币跨国支付清算体系，从而适当缓解主权货币主导下的传统货币体系缺陷，也有助于应对全球“流动性困局”。英国央行计划发布由中央机构控制的类比特币数字货币RSCoin。这是一款完全基于央行的需求来设计的基于区块链技术的数字货币。该技术将依赖于一系列权威机构，如商业银行，防止货币重复消费。我国央行也在研讨发行数字货币方案。

由于任何人都能创造自己的区块链系统：启动条件十分简易，且不难实现。当前正迎来区块链的寒武纪大爆发，大量区块链开源或封闭试验得以实施。现有区块链林林总总，有公有链、联盟链与私有链之分。知名项目除了R3CEV，还有Linux基金会推进的超级账本

（Hyperledger），以智能合约平台而著称的以太坊，以及基于比特币区块链系统的闪电网络与侧链技术.....正如区块链数据的合法性是以算法来竞争最长链，这些区块链协议与技术也呈现出非常激烈的竞争局面，它们最终哪一种会胜出，联盟链与公有链哪一个笑到最后，并成为互联网通用价值传输协议，目前还是个谜。

或许，互联网的早期发展能带给我们以启示。互联网鼻祖是美国国防部的军用网，叫做“阿帕网”（ARPAnet）。在20世纪70年代，ARPAnet已经形成好几十个计算机网络，但是每个网络只能在网络内部的计算机之间互联通信，不同计算机网络是一个个信息孤岛，它们之间不能通讯。直到1974年，研究人员设计了连接分组网络的协议，其中就包括著名的TCP/IP——网际互联协议IP和传输控制协议TCP，这才将这些孤岛连通起来，构成现在的因特网（Internet）。因而，联盟链与公有链之间，比特币与以太坊之间，以及其他区块链网络之间，也许并不是一个你死我活、赢家通吃的局面，而是会通过构建不同区块链之间的价值传输协议，而形成一个统一的区块链：互联链（Interchain）。同样，互联链也会像互联网的物理层、网络层、传输层、应用层的层级设计一样，根据功能定位的不同、应用场景的不同、共享账簿的开放权限的不同，而演化为不同层级的协议。

如果说TCP/IP协议让我们进入了信息自由传递的时代，区块链则将把我们带入价值高速公路时代。区块链协议的完善，将构成共享金融的基础设施。当今互联网正进入分布式时代，逐渐从传递信息的互联网演变为交换价值的互联链。出于价值交换的需要，人类进入数据可计算时代。数据结构也进化成为附带计算机程序的代码，数据可以自我计算，自我运行，从而成为智能数据，为整个人类社会进入智慧社会打开了大门。

[1] 作者为中国人民银行金融研究所所长。

序二

区块链：网络世界运行规则与技术的全新探索

王永利^[2]

近年来，区块链成为全球互联网领域，特别是金融互联网界快速升温、越来越热的概念。在中国，区块链更是引发越来越多的人、越来越热的关注和探索。

区块链最早面世，是由于2009年初发布的比特币，区块链成为比特币产出、记录、流通的基础协议和技术应用。尽管比特币自面世以来饱受争议，甚至仍不能被政府和货币当局视同为“货币”，但比特币所应用的区块链技术却得到了包括政府和货币当局在内的广泛关注。

为什么区块链会成为快速升温的热点技术和话题？

这其中最重要的可能就是，在区块链技术基础上推出的比特币，开启了一种与传统社会（线下）没有多少关联的，完全应用于网络世界（线上）的网民身份验证、财富确认、交易记录、公证核查等全新的技术与规则体系的探索和尝试，而这给人们适应互联网社会的发展提供了可选路径和无限遐想。

从其在比特币的应用情况看，区块链直观讲，就是将加密技术与互联网技术相结合，所形成的一套全新的数据区块（Block）建立、比特币发行分配、网络身份验证，以及挖矿所形成的比特币（价值）确认、比特币交易记录，比特币的链上流动（价值转移），以及加密（加入了

区块与交易时间标识等因素）登记和查验核实等在内的互联网协议规则和账本（Ledger）体系。

正因为比特币并不是线下法定货币的替代物，而是非法定货币当局发行和管理的，主要模仿黄金的模式，完全由互联网基础协议和严格的加密技术保护和支持的、全新的、去中心化的网络货币（虚拟货币），由此也形成了一套不同于、也不受制于现实社会法律的新的货币规则和体系，并且可以与法定货币进行买卖或兑换。

比特币自推出以来已超过8年时间，没有出现过资金或用户信息被盗用的记录，其安全性得到验证，而且其资金清算的效率和成本也具有明显的优势。这使得人们对比特币所应用的区块链技术的信心不断增强，而且人们也越来越清晰地认识到，区块链尽管是比特币所首创和应用的一种技术和协议，但区块链并不等同于比特币，其应用也绝不会只局限于比特币。区块链的应用，可以是去中心化的，也可以是中心化的；可以是公有链模式，也可以是私有链模式。因此，在比特币之后，区块链技术也在不断发展创新，并不断探索新的应用领域。

区块链之所以被越来越多的人高度重视，是因为互联网的发展和广泛应用，已经使得越来越多的经济交往和交易活动转到网上进行。网络世界（或线上社会）正在快速扩展、充实和活跃，而网上交易必须解决当事人的身份验证、价值核实、交易记录、查验核实等方面的效率和安全保护问题，需要严格的中介和协议（规则或宪法）。在这方面，传统思维和习惯做法就是顺应线下交易向线上转移的发展轨迹，将现实（线下）社会的通行规则和做法推到线上（网络）社会，但实践中却越来越难以适应网上交易的需求。

比如，当事人身份验证，自然的选择就是以各国法律保护的身份证件的信息为基础，再增加账户或交易密码，以及脸谱、虹膜、指纹等生物识别等，进行线上交易的身份验证。这种方法，首先就使得跨境互联互通的网络世界的公民身份信息受到现实社会行政管辖的制约。同时，

非数字化的、多种身份信息的采集和验证会大大增加成本、降低效率。

再者，现实社会中各种经济活动涉及资金清算的，除直接的现金交易外，都需要当事人首先在银行等机构开立账户，并通过开户机构进行资金清算。但由于种种原因，即使一个国家内，也不可能要求所有的公民都在一个开户机构（包括其分支机构）开立账户，跨国之间就更不可能做到。这就使得在不同机构开立账户的当事人的交易，必须通过其开户机构之间的清算才能完成。将这种模式推行到网络世界，更将严重影响交易确认和资金清算的效率和成本。

还有，现实社会中，交易活动的计价和清算必然涉及货币，而货币都是以国家或地区主权保护的法定货币。在互联网跨境互联互通，互联网交易跨境发展的情况下，交易的计价和资金的清算还涉及货币的问题，多种货币的运行，也将大大增加清算的成本和风险。

因此，网络世界和网络交易的发展，亟须与之相适应的身份验证、价值核实、货币计价、交易确认与记录、账户管理与核查等方面的创新。而区块链技术为此提供了非常重要的启迪和实践。

当然，比特币的应用是一种极端的例子，最初始的比特币并不是法定货币可以直接转化出来的，而是要在网络世界通过“挖矿”才能获得的。因此，比特币可以完全撇开线下社会规则，运用区块链技术形成一套全新的游戏规则，并由线上向线下延伸。而现实社会中，无论线上还是线下交易，其主体都是人（包括法人），其财富或价值的管理不应该被完全分割，而必须连接和融合，因此，O2O是必须的。这就要求区块链的应用，不仅要研究和解决网络世界的问题，还要研究和解决网络世界与现实社会的连接与融合问题。这将带来更多的挑战和风险，也需要更多的人、更大的力量、更深入的探讨和创新。也可能未来区块链技术会被更先进更完善的技术所替代，但区块链的历史价值将是不可磨灭的！

为普及区块链的知识，引导区块链的研究，推动区块链的应用，最近我国一批对区块链理论研究和应用实践颇有造诣的专家学者，将其心得和成果精心梳理，编写出版了《区块链：从数字货币到信用社会》一书，非常值得认真阅读。当然，区块链作为一个全新的技术和概念，其研究和探索才刚刚开始，希望《区块链:从数字货币到信用社会》一书能够成为大家学习、研究区块链的“垫脚石”，也希望作者们能不断推出新的成果和作品！

[2] 作者为乐视金融CEO、中国银行原副行长。

序三

区块链——未来全球信用的基础协议

韩锋[\[3\]](#)

在2015年的时候，阿里巴巴研究院和中国社科院金融所举行了一个研讨会，我受邀前往。会议的主旨很宏大，提出要为互联网金融建立一个理论体系！围绕这个主题，诸多中国一流的学者提出了自己的观点。我也深受启发，尤其是随着最近几年来区块链技术的兴起，似乎给这一目标找到了答案。在探讨区块链能给互联网金融带来什么之前，让我们先看看究竟互联网会为金融带来什么。

金融的核心无疑就是“信用”的建立。最原始的商品经济是以物换物。但大家很快发现这样的交易成本很高。如果你把几车皮商品拉去，但是交易没做成，还有可能被土匪抢了，不仅交易成本高，还要面临很高的风险。所以大家考虑，要让市场经济更好地发展，首先要降低交易成本。于是很快就过渡到了利用信用建立交易的方式。信用的建立才是金融的核心。当然，我们传统的信用建立无疑是靠很多的“中心”，譬如央行、商业银行，要有法院、经济警察等。但是传统金融的问题就是成本过高。我本人很喜欢在北京周边骑车，只要骑车超过一百公里，虽然只是到了北京的郊区，但金融生态就已发生了巨大的变化！我就经常找不到ATM（自动取款机）机了，找不到银行网点了。我自己是不太爱带现金的，结果有一两次在北京郊区把我弄得既不能住店，也不能吃饭，甚至无法买水。

打个比方，这就像人的身体，只靠主动脉无法到达全身，一定要有毛细血管，才能让身体的很多地方得到营养。如果人的毛细血管出了问

题，那么你这个人就会得各种病，非常严重。所以互联网金融第一步搞得风风火火的，实际上是“支付宝”们，它向前跨的一步就是依靠大数据来建立信用，这是前所未有的。在我创业的时候，我也曾经去银行贷过款。其过程非常烦琐，要调查你的资产情况，恨不得把你的家底全搞清楚，之后才决定是否给你贷款。据说当时银行里所谓的小额贷款是五百万元。为什么这么大的数额？因为成本下不来。所以光靠银行是不行的，不说我去山沟里没ATM，很多中小企业甚至都无法得到贷款服务。结果突然出现了支付宝、余额宝，“信用”是建立在互联网交易的大数据基础上，这就是一大突破！大数据金融基本上是建立互联网金融的第一步。它让信用建立的成本比传统银行吸储放贷方式的成本下降了很多。后来出现了P2P（点对点）、众筹等，都促使信用建立成本下降成为趋势。

那为什么还需要区块链？因为光靠互联网公司大数据产生“信用”是远远不够的，让我们看看传统金融出现的几个问题。

首先，互联网公司的大数据实际形成了数据孤岛。每个互联网公司都会提倡互联网的共享、公开、透明精神。但事实上，他们会将掌握的大数据与他人共享吗？目前，答案是否定的。在当前形势下，大数据必然是每一个公司的绝对内部资源，不可能进行无边界的共享，这就出现了“大数据集中”的问题。

这样一来，互联网发展到现在就出现了一个悖论，走向了初衷的反面。大数据的集中会引起富者越富的马太效应。如果形成数据孤岛，大数据资源集中到少数人手中、全社会无法形成环流，这些宝贵的数据资源只能为少数数据的掌控者所利用，用户个人作为大数据产生者完全没有获得信用资源的主动权，这非常不利于全球市场信用成本的进一步下降。

其次，数据所有权现在是错配的。海量数据是由每一个参与主体产生的，尤其是在腾讯微信这样的软件上。但大数据的所有权属于每一个

参与主体吗？参与主体可以管控自己的大数据吗？答案也是否定的。尤其是2016年初发生了一件恶劣的事情——“百度卖吧”事件。在百度上形成一个“吧”产生的数据、资源的所有权应该归属于用户，这其中包括“吧主”也是由参与用户选举产生的。但是，百度却能将产生的大数据效益公开出售！

同样，在微信上我们每天能产生多少数据？我们每天产生的社交、交易数据本应该是完全属于产生者每一个人的。如果按互联网共享、平等、透明的精神，这种大数据产生的是一种“全球性的信用资源”。

所以，新的创新一定是要解决的问题是：大数据既要能够共享，又要能够清晰所有权归属。表面上看，这两点有些矛盾。众所周知，第一代互联网解决了信息的自由传递问题。“信息”本身可以复制、多次传递并且免费，这都没有问题。但“资产”不可以。在现实中，“资产”在传递过程中所有权唯一，资产的所有权是不能随便复制的。所以，如果按第一代互联网TCP/IP协议做的话，大家似乎无法在互联网上建立所有权和信用制度。因为资产属性一定是唯一的，不能说拷贝就拷贝。如果任何一个所有权可以无限复制，就没有任何人愿意相信，也就没有任何信用可言了。

2008年比特币的诞生让以上两个问题迎刃而解。中本聪认为不能靠某个中心建立信用。因为任何过度中心化的结果都会产生信息不对称，会存在利用中心权力损害参与者的利益、损害市场上其他方利益的情况。所以，比特币白皮书开宗明义地提出：我们要开创一种不需要第三方的、不需要中介的支付系统，即电子货币的支付系统。但这首先要解决资产所有权唯一性的问题，即不能重复支付。否则，这个所谓的电子货币无外乎就是存储的数字，如果还是可以无数次拷贝是没有任何信用价值的。在此之前，很多人也尝试建立电子货币系统。类似“Q币”显然是依靠腾讯公司发行的，一旦腾讯公司垮了，Q币则一文不值。但中本聪宣称要创造的这个P2P电子货币支付系统不相信任何中心、不需要任

何第三方！

比特币的解决方案就是我们现在讨论的区块链技术。第一个也是最核心的概念是“时间戳”。“时间戳”本身不是中本聪发明的，早就有国家的“时间戳”中心。比如一个合同，可以盖一个“网络时间戳”，相当于一个证明。即在这个时间点，合同的文本已经形成，当出现纠纷的时候，可以利用这个证明来打官司等。比特币系统的每笔交易，为了防止重复支付，都盖了“时间戳”。因为盖了“时间戳”以后，同一笔资产就不能支付给第二个人了。如果有人重复支付，那么时间会对不上，系统会自动识别为非法交易。唯一的合法交易只能是盖了“时间戳”的那笔，这就成功解决了重复支付的问题。这个办法听起来可以解决重复支付问题，证明了此时此刻财产转移的唯一性，但问题是：谁来盖这个“时间戳”？中本聪显然是市场的信徒，信奉亚当·斯密提出的市场都是由自利的人组成的，要有一定的利益规则。盖“时间戳”的是所谓的“矿工”。矿工每10分钟给全网的每一笔交易盖“时间戳”——记账。他们也是有利益驱动的。矿工的利益是币基所产生的新币的奖励，通过竞争到一段时间内（约10分钟）的唯一合法记账权而获得，谁竞争到了，谁就可以获得一定数量比特币的奖励，同时，全网其他矿工要同步一致它这个记账，然后竞争下一个区块记账权。最初，这个奖励是50个比特币。按照规则设定，每四年减半一次。2013年减半到25个比特币。所谓区块链，就是这样一个又一个区块账簿连接起来形成的单向记账链条。

比特币的区块链是靠消耗计算资源给全网作证，重新建立信用体系。大家经常看到网上的讨论，比如，下一代微信可能是什么，下一代淘宝可能是什么等。在我们看来，下一代最有可能的是一个真正去中心化的系统。每个人在微信上产生的大数据，对每个人自身都有很大价值。如果这些数据用类似Factom（公证通）这样的系统加密后形成一个新的数字水印（哈希）然后保存在比特币的区块链上，每个人自己产生的大数据都不可篡改，私钥掌握在每个人自己手中，也就掌握了自己大数据的所有权。当我们任何人需要向银行贷款时，只要提供自己的公钥

和私钥给全球任何一家银行，根据大数据分析就可以得出贷款人的信用情况，这就可以让每个人通过大数据+区块链获得全球信用。

阿里巴巴副总裁高红冰对我说：“传统金融的信用建立在钢筋水泥的大厦上，你看银行是不是都得盖大楼？但未来的信用是建立在区块链的数据上。”所以区块链就是靠全网分布记账，自由公证，建立了一个共识数据库，这就是未来信用的数据大厦。

畅想一下未来，比如说原来你的出生证、房产证、结婚证等，需要政府备书，好像政府才能承认。但一旦跨国，你就会遇到很多麻烦，包括合同。跨国以后合同可能就不能被承认了，或者无法执行。整个传统的信用执行系统成本非常高。这些成本都摊在了我们每个人的头上。但是，如果全网公证帮你证明，几乎无法作假。否则就像我刚才说的改时间，除非我有本事把每个人的手表都改了。将来大家公证一件事情，比如公证你们的情侣关系，一下子就会成为全网的事实，修改的话几乎是不可能的了，除非到全网的每个矿工那里去改，成本高到无法接受。现在，要想修改的话，我问过比特币的矿工，如果他们的世界想要这样篡改区块链上的数据，成本是十几亿人民币（随着时间还在迅速地增加）。成本一旦高了，大家就都不想作假了，因为付出的代价和获得不成比例。

一个新的时代，未来的信用、真假是靠全网公证某个协议，靠全网每台电脑成为记账人来实现的。这在人类历史上打开了广阔的空间。它解决了什么问题？未来信用由每个消费者自己靠大数据在区块链上产生，就像北京市金融局霍学文书记所说的，“区块链会成为全球金融的基础架构”，这是未来的信用大厦。

[3] 作者为清华大学博士生，iCenter导师，比特币基金会终身会员，曾任清华大学十五规划重点课题“基于网络(大数据)的创新人才评价和选拔”项目负责人，美国甲骨文教育基金会中国合伙人。

第一章

区块链创世纪^[4]

一、先驱篇

（一）中本聪的生日

P2P Foundation是中本聪发布比特币白皮书的网站，注册这个网站必须提供出生日期，中本聪填写的是1975年4月5日。当然，没有人会认为这些信息是真实的，但如果认为这些信息是随便填的，又似乎低估了一位密码学家的自我修养。

4月5日在货币史上是具有重要意义的一天。在1933年的这一天，美国总统富兰克林·罗斯福签署了政府法令6102，该法令规定所有美国公民持有黄金都是非法的。

罗斯福没收美国人的黄金，并以美元交换，然后让美元贬值了40%，强制推高黄金价，目的是让美国的债务贬值，从而对抗大萧条。这些措施造成的后果是美国人的财富被洗劫了40%。

有许多人认为这是美国政府所作所为中最违反宪法的行为之一。这是政府不经过民主程序对民众最直接的盗窃行为之一。

那么，在1975年又发生了什么？在1975年，福特总统签署“黄金合法化”法案，美国人可以再一次合法地拥有黄金。

这两个数字撞在一起实在太蹊跷，无法让人不怀疑这是有意为之。

毕竟中本聪没有说他出生于1933年，而是说1975年。因为如果出生年份是1933，这意味着当他发明比特币时已经75岁了，显然不太可能。假如1975年出生，2008年时他33岁，这明显地更让人信服^[5]。

如果仔细研究中本聪的创世论文以及比特币代码，一定对他注重细节以及对货币知识的掌握感到惊讶，显然，他的生日数字不是随机组合。没错，这是一个政治隐喻，透露给关心这些细节并能理解的特殊人群，比如那些密码朋克们。

（二）密码朋克

基于密码学技术的比特币，并非加密货币之发轫，早在20世纪80年代，密码朋克就有了加密货币的最初设想。蒂莫西·梅（Timothy May）提出了不可追踪的电子货币——加密信用（Crypto Credits），用于奖励那些致力于保护公民隐私的黑客们。

加密货币的难点在于如何建立分布式共识，也就是莱斯利·兰伯特（Leslie Lamport）等人1982年提出的拜占庭将军问题（Byzantine Generals Problem）。所谓拜占庭将军问题是指，把战争中互不信任的各城邦军队如何达成共识并决定是否出兵的决策过程，延伸至计算领域，试图建立具有容错性的分布式系统，即使部分节点失效仍可确保系统正常运行，也可让多个基于零信任基础的节点达成共识，并确保信息传递的一致性。

1990年，大卫·乔姆（David Chaum）提出注重隐私安全的密码学网路支付系统，具有不可追踪的特性，就是后来的电子货币Ecash。不过Ecash并非去中心化系统，后来大多数电子加密货币都继承了Ecash重视隐私安全的特性，以盲签名技术（Chaumian blinding）为基础，但都没有流行起来，因为它们都依赖于一个中心化的中介机构。

1993年，埃里克·休斯（Eric Hughes）和其他几个人创建了一个“密

码朋克邮件名单”的加密电子邮件系统，简称“密码朋克”，对抗受到政府监控的互联网电子邮件。埃里克·休斯在《密码朋克宣言》里阐述了密码朋克的使命与目标。

“密码朋克致力于建立匿名系统……电子时代，隐私是开放的社会不可或缺的……我们不能期望政府、企业或其他大型的匿名组织保障我们的隐私……如果期望拥有隐私，那么我们必须亲自捍卫之。我们使用密码学、匿名邮件转发系统、数字签名，以及电子货币保障我们的隐私。”

密码朋克在20世纪90年代最为活跃，包括电脑黑客、密码学家和追求隐私的狂热者，他们极力主张用密码技术保护个人隐私不受其他人或者政府的侵犯，但在当时，密码技术并没有在日常生活中得到广泛应用，而是被政府垄断，主要用于情报和保密。

密码朋克们意识到密码学对社会经济的深远影响，蒂莫西·梅说：“正如印刷技术改变了中世纪的行会及社会权力结构，密码技术方法也将从根本上改变机构及政府干预经济交易的方式。”

比特币的加密理论基础来源于以下几项密码学的技术创新：1976年威特菲尔德·迪菲（Whitfield Diffie）与马蒂·赫尔曼（Marty Hellman）发明的非对称加密算法，1977年罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adelman）率先发明的第一个具备商业实用性的非对称RSA加密算法^[6]，以及1985年由尼尔·科布利茨（Neal Koblitz）和维科特·米勒（Victor Miller）首先提出的椭圆曲线加密算法（ECC）。这些加密算法奠定了现在非对称加密理论的基础，被广泛应用于网络通信领域。

但是，当时这些加密技术发明均在NSA（美国国家安全局）严密监视的视野之内。NSA最初认为它们对国家安全构成威胁，并将其视为军

用技术。直到20世纪90年代末，NSA才放弃对这些技术的控制，RSA算法等非对称加密技术最终得以走进公众领域。

有趣的是，中本聪并不信任NSA公布的加密技术。2013年9月，斯诺登爆料NSA采用秘密方法控制加密国际标准，比特币采用的椭圆曲线函数可能留有后门，NSA能以不为人知的方法弱化这条曲线。所幸的是，中本聪使用的不是NSA的标准，而是另一条鲜为人知的曲线。全世界只有极少数程序躲过了这一漏洞，比特币便是其中之一。

1998年，另一名密码朋克戴伟（Dai Wei）提出了匿名的、分布式的电子加密货币系统——B-money。分布式思想是比特币的重要灵感来源，在比特币的官网上，B-money被认为是比特币的精神先导。

B-money的设计在很多关键的技术特质上与比特币非常相似，但是不能否认的是，B-money有些不切实际，其最大的现实困难在于货币的创造环节。

在B-money系统中，要求所有的账户持有者共同决定计算量的成本并就此达成一致意见。但计算技术发展日新月异，而且有时并不公开，计算量的成本这类信息并不准确、及时，也难以获得，因而B-money很难成为现实。

2005年，尼克·萨博（Nick Szabo）提出比特金（Bitgold）的设想：用户通过竞争解决数学难题，再将解答的结果用加密算法串联在一起公开发布，构建出一个产权认证系统。该系统已经非常类似于比特币的理念，且发布日期与比特币非常接近，所以，萨博也被视作中本聪的潜在候选人之一。除此之外，萨博还发表了许多关于《合同法》在网络中安全实现的理论文章，这些思想被视为区块链智能合约的起源。

但萨博终究不是中本聪，他擅长于理论研究而不是编程实现，他一直寻找能将比特金变为现实的开发者，但没有人响应。

从乔姆的Ecash，到戴伟的B-money，再到萨博的比特币.....几代密码朋克都怀着对自由货币的向往，像堂吉诃德一般偏执而骄傲，试图征服加密货币的风车，最终都功亏一篑，这些理论探索并未真正进入应用领域，长期不为公众所知，但他们的研究成果加速了比特币面世的进程。

（三）加密货币的乔布斯

非对称加密技术的发明以及创立Napster^[7]的肖恩·范宁（Shawn Fanning）与肖恩·帕克（Shawn Parker）点对点网络技术的开发，使比特币的出现成为可能。通过这两项技术，可以建立分布式交易账簿，并以呼叫问答机制向全网广播，网络节点不停地检查接收的数据，避免数据被篡改。

数字货币的诞生历程就像是一次扣人心弦的橄榄球进攻，在乔姆、戴伟、萨博等“明星球员”的冲刺下，每一次冲阵都前进了一些，但离“达阵”总还差一点距离。

最后的难点就是“双重支付”问题。“双重支付”阴云在数字货币诞生伊始，就始终盘桓不去。其实解决方法是现成的，就是亚当·拜克（Adam Back）在1997年发明的哈希现金（Hash Cash）算法机制。但起初，该设计是用于限制垃圾邮件发送与拒绝服务攻击。这就好比另一个球场正进行着田径接力赛，并没有引起橄榄球赛场的注意。2004年，哈尔·芬尼（Hal Finney）接过拜克的接力棒，将哈希现金算法改进为“可复用的工作量验证（Reusable Proofs of Work）”。他的研究又是基于达利亚·马凯（Dahlia Malkhi）与迈克尔·瑞特（Michael Reiter）的学术成果：拜占庭容错机制（Byzantine Quorum Systems）。

所有的技术都已成熟，终于由中本聪在2008年完成“达阵”。他将RPOW（可复用工作量验证）引入加密货币，就像博尔特跑入了橄榄球

赛场一样，一下发挥出巨大的威力，比特币诞生了。中本聪阐述了RPOW机制如何用于解决拜占庭将军问题，RPOW消除了中枢“时间戳”服务器的需求，杜绝了那些不怀好意的人通过攻击中央服务器进行比特币无限重复消费的问题。

非对称加密、点对点技术、哈希现金这三项关键技术没有一项是中本聪发明的，但最后摘取桂冠的却是他。这与其说是运气，不如说是因为中本聪恰好具备发明比特币的全部素养：既是“橄榄球员”，又是“田径高手”，更关键的是他还是编程大师，能够把自己的想法付诸行动。中本聪就像是加密货币界的乔布斯，纵横于不同领域，采撷各家之长为我所用。

正如戴伟事后评价说：“要想开发出比特币，必须：①对货币有非常深入的思考；②要了解密码学；③认为比特币这样的系统从理论上是可行的；④要有足够的动力将这个理念开发成实际产品；⑤编程能力出色，能保证产品安全；⑥有足够的社交技巧，才能围绕这个产品建立一个成功的社区。密码学圈子能符合前三个条件的人就已是凤毛麟角。”

（四）创世区块

中本聪第一次出现是在2008年11月1日。那一天，秘密讨论群“密码学邮件组”里出现了一个新帖子：“我正在开发一种新的电子货币系统，采用完全点对点的形式，而且无须受信第三方的介入。”该帖的署名就是塞托西·中本聪（Satoshi Nakamoto）。

这样的电子货币系统是密码朋克们数十年来的梦想，有许多人进行过尝试，但都失败了。当时最积极的反应也只是持怀疑态度，因为密码组成员已经看过太多低水平的新手想出来的宏伟计划，他们的本能反应就是怀疑。当时有不少人表示，这样的系统是不可能实现的，连大卫·乔姆这样的密码学天才都失败了，更何况一个无名小辈呢。

中本聪细致入微地回答了所有疑问，最终在白皮书中提出了一个可行的方案。白皮书遵从学术习惯采用“我们”作为第一人称，行文也是标准的论文格式。

“本文提出了一种完全通过点对点技术实现的电子现金系统。它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。”

中本聪选择在2008年全球金融危机的时候将比特币公布于世，在介绍他的创新时说道：“传统货币最根本的问题在于信任。中央银行必须让人信任它不会让货币贬值，但历史上这种可信度从来都不存在。银行必须让人信任它能管理好钱财，并让这些财富以电子货币形式流通，但银行却用货币制造信贷泡沫，使私人财富缩水。”

与密码朋克的文章相比，比特币创世论文的语言显得格外冷静和去政治化，文中没有出现政府或主权的字眼，仅将比特币描述成一个区别于传统金融的支付系统。

两个月之后，也就是2009年1月3日，中本聪发布了开源的第一版比特币客户端，宣告了比特币的诞生。他同时通过“挖矿”得到了50枚比特币，产生第一批比特币的区块就叫作“创始区块”（Genesis block）。

在全球金融危机时期，中本聪将他的怀疑和愤怒集中在了银行机构上，但与用生日密码挖苦美国政府一样，他不动声色地幽默化了英国财政大臣达林一把，在创世区块里写道：“当时正是英国财政大臣第二次出手疏解银行危机之时。”

财政大臣左支右绌的窘态就这样被永久记录在区块链上。“第二次”在此与其说是一个量词，不如说是一个形容词，很形象。

9天以后，中本聪向密码学家哈尔·芬尼转账了一笔比特币。那笔转

账在当时还不值一文，却在加密货币篇章里留下浓墨重彩的一笔。这是人类历史上第一次摆脱受信第三方金融机构而完成的点对点交易。

与许多患有隐私癖的黑客一样，中本聪也是独行侠。他几乎没有合作伙伴，如果非要说一个，哈尔·芬尼勉强算半个。芬尼是参与过PGP加密技术研发的一位顶级开发者，也是密码朋克的重要成员。当中本聪在加密邮件列表中宣布比特币的想法时，迎来的更多的是冷嘲热讽，但只有芬尼热情支持。芬尼很早就对加密货币计划感兴趣，早在2004年，他就推出了自己设计的加密货币，在其中采用了可重复使用的工作量证明机制，所以他明白比特币的价值。当中本聪公布第一个版本的软件时，芬尼马上下载并测试。

多年后，芬尼在社区回忆这段经历说：“我想我是除了中本聪以外第一个运行比特币的。我开采了大约70个块，而且我还是第一个比特币交易的接受人，中本聪测试时转给了我10个币。在接下来的几天里，我和中本聪通过邮件谈了很多，主要是我报告一些故障然后他把它们搞定。”

社区网友亲切地把芬尼称作“中本聪的沃森”，因为当电话被发明时，第一个电话就是贝尔打给他的助手沃森：“沃森，快过来，我想见你。”2014年8月，在与渐冻人症搏斗了五年之后，哈尔·芬尼在亚利桑那州去世。向“沃森”致敬！

（五）后起之秀

比特币发布后取得了空前的成功，媒体与公众纷纷把中本聪与20世纪90年代的那些密码学天才们相提并论。中本聪对此不以为然。

尽管维基解密创始人朱利安·阿桑奇（Julian Assange）^[8]宣称比特币是从密码朋克中来的，中本聪却对密码朋克或者密码无政府主义只字不提。

2010年，维基解密宣布接受用比特币的捐款时，社区一片欢呼，中本聪却出人意料地提出了反对意见：

“不，请不要揠苗助长。比特币这个项目需要平静地成长，这样软件才能够逐渐强化。我请求维基解密现在不要使用比特币。比特币还是一个非常小的测试项目，还处在婴儿期。在这个阶段，你们所带来的关注将摧毁我们。”

中本聪对20世纪90年代的失败者记忆犹新。他指出Beenz（虚拟货币）、Flooz、Ecash（电子货币）等数字货币先驱失败的根本原因就在于其中心化的架构。因为一旦为数字货币信用背书的公司倒闭，或保管总账的中央服务器被黑客攻破，该数字货币就会面临信用破产和内部崩溃的风险。

2013年，一名叫特拉梅尔的安全研究人员公布了他与中本聪的加密邮件往来。在邮件中，中本聪写道：

“我觉得现在更多的人对90年代感兴趣，但是经过数十年，我们已经看到了基于‘信任第三方’系统的失败（例如Ecash）。我希望人们能够有一种区分，即知道：我们是在尝试首次建立一个以‘非信第三方’为基础的系统。”

然而，要向公众解释这两者的区分很难，有一次他在论坛抱怨：“向普通读者描述比特币真是‘bloody hard’（该死地困难）。”^[9]

中本聪对加密货币前辈的态度难说有几分尊重，但世道轮回，没过几年他也面临后起之秀的挑战。

对比特币的共识机制来说，挖矿是必须的。正如白皮书中开门见山指出的：“想要在点对点（P2P）基础上布置一个分布式的‘时间戳’服务

器，我们必须使用一种与亚当·拜克的哈希现金相似的工作证明系统。”

但很多人都认为，比特币网络消耗的庞大计算力是一场能源灾难。素数币创始人萨尼·肯（Sunny King）试图将算力应用于蛋白质折叠、寻找素数这样的科学工程。他自信地写道：“加密货币目前已分道扬镳为两条道路：一种是能源密集型，另一种是环保节能型。我相信，在未来较长一段时间（5年以上），环保节能型货币将因其成本优势而挑战能源密集型货币。素数币第一次引入非哈希现金的工作量证明机制，使算力不仅用来制造区块链，还提供额外的潜在科学价值。”

除此之外，Sunny King还发明了权益证明（PoS）。与要求矿工证明执行一定量的计算工作不同，权益证明要求用户提供证明一定数量加密货币的所有权即可。

还有一些人对比特币处理交易的效率很不满意。比特股创始人拜特·马斯特（Byte Master）在社区发帖：“互联网带宽、CPU（中央处理器）、硬盘空间等都是非常宝贵的资源，指望用户用个人时间和挖矿的方式获得财富，这对于创新而言将是不利的。此外，比特币10分钟的确认时间对于验证付款而言实在是太长了，它应该像如今刷信用卡那般迅速。”

中本聪是这样解释的：将来用户只需运行轻节点，只交易，不挖矿，处理区块的节点将是矿场部署的大型服务器。最后，他无奈地说：“如果你没有理解我的意思，我没时间说服你。”在心底，恐怕他又吐槽一遍“bloody hard”吧。

另一位技术天才维塔莱克（Vitalik）从未在社区与中本聪对过话，毕竟在2008年的时候，他才13岁。Vitalik与中本聪的交流更多的是通过代码。他指出，中本聪作为一个老派C++程序员，编程水平并不高明，但运气不错：“虽然中本聪在2008年为比特币做出的绝大多数决策我们仍坚持着，但他的选择绝对不是完美的，幸运的是他正确的次数经常比

错误要多。事实上有几个实例，因为中本聪的选择我们获得了更好的结果。”

他说的是中本聪在比特币的代码中埋下的三个“彩蛋”，后来被证明都是对的。

第一个是比特币使用公钥的哈希作为地址，带来了不必要的复杂度和浪费。但事实上，这是深思远虑的未雨绸缪，因为可以让比特币完全免受量子计算机的威胁。第二个是比特币总量2100万的限制，或者说是2的50.899次方。这是一台计算机里面能以标准整数形式存放的最大整数，超过那个值的话，数值将像里程表那样归零。第三个是选择了正确的椭圆曲线，成功绕开了NSA居心叵测的陷阱。

中本聪在代码里处处留情，可惜能读懂他的人不多。很难说Vitalik能否算是一个知音，因为后者并不认为中本聪天才地设计了这一切，他说：“这些设计带来更好结果的原因可能连中本聪自己都没想到过。”他认为中本聪是蒙对的。2014年，他发起以太坊项目，试图以一套图灵完备的脚本语言，解决比特币扩展性不足的问题，提供不同智能合约，让用户搭建各种应用。有意思的是，以太坊以加密货币先驱的名字作为货币单位，戴伟、萨博、芬尼均名列其中，唯独没有中本聪。

2010年12月12日，中本聪在比特币论坛发布了他的最后一个帖子，其后，他在网络上的公开活动频率也逐渐降低。直到2011年4月，他发布了最后一项公开声明，宣称自己“已经开始专注于其他事情”。他依然跟几个关键人物保持着联系，比如说比特币的首席开发者加文·安德森，并提出了一些建议。但到这一年年末，安德森公开表示，中本聪回复他电子邮件的次数越来越少，然后慢慢地就再也没了消息。

二、货币篇

（一）石币之岛

密克罗尼西亚是太平洋的三大岛群之一，其中最西边的雅浦岛上曾住着一群非常古怪的土著居民。1903年，美国的人类学家威廉·亨利·弗内斯（William Henry Furness）在雅浦岛住过几个月，并把他在当地所见的风俗记录成书，书名叫《石币之岛》，因为当地的货币体系令他印象深刻。

雅浦岛上没有金属资源，于是石器在他们的文化中扮演着重要的角色。但即使是石灰岩，也需在离雅浦岛400英里远的帕劳岛上才能找到。雅浦岛部落里的探险家们开采这些石灰岩，打制成内部中空外部呈环形的石轮，然后用木筏运回雅浦岛作为货币使用。这些石轮小的直径30多厘米，大的直径有3米多。为了便于运输，有时会往中间插一根粗壮の木柱。

雅浦石币有个很有趣的特点。交易双方在决定了使用多大的石币付费后，如果那个石头太大了，不方便运输，那么卖家只要在买家的石头上做个标记就可以了，这样就算是付费了。那个标记就说明这个石头已经属于卖家了，而石头仍然躺在买家屋里。

不只如此，还有更神奇的事情。岛上有一户大财主，所有人都承认他们家是首富，但奇怪的是，没有人见过首富家里的石币，连他的家人都没见过。他们家拥有的财产是一个巨大的石币，大小只有祖辈才知道，因为这个石币一直沉睡在海底。原来许多年以前，这户人家的祖辈和其他人外出探险，寻找和开采石灰岩，就像美国西部的淘金客一样。他们的祖辈运气不错，碰到了这个庞然大物，便将其制成石币，然后用木筏拉回家。但是归途中遭遇了强烈的暴风雨，为了逃命，探险队只好砍掉拉筏的绳子，于是那块巨大的石币沉入了大海，永远也找不回来了。回村后，探险队的成员都替他作证，那块石币尺寸巨大并且质量上乘。虽然已掉落大海，但大伙都见证了这块石头的去处，所以不会影响

它的价值。它的主人仍然可以用它买东西，就跟把石币运回家存放起来的效果一样。

如果这个还不足以让你惊讶，请看下面的故事。雅浦岛岛民都不穿鞋，并且也没有发明轮子，自然也就没有车道。岛上只有一些适合原住民裸足行走的珊瑚礁道路，但是西方殖民者却要求他们修筑能行驶汽车的公路。德国在1898年从西班牙手中买下了这座岛，要求几个部落的首长组织修路。修路对土著居民而言完全没有意义，德国人的马克在土著居民看来跟废纸差不多，所以命令下达了几遍都无人搭理。想想也是，一伙拿枪的人登上一座自己从未踏足的岛屿便声称拥有岛屿的所有权，还强迫当地居民为自己修路，这不是流氓是什么。德国政府研究了雅浦岛的文化习俗后，突然开窍了，下令对几个违抗命令的部落征税。他们派人到这些部落的每家每户，并往他们最珍贵的石币上涂上黑十字标记，声称这些石币已经归德国政府所有了。这个解决方案既简单又“文明”——文明用在这儿真够讽刺的——但的确非常奏效，可谓是“取之于无形，使人不怒”。所有人都觉得政府抢了自己的钱，为了使钱不被抢走，只得乖乖去替政府修路。最后路修好了，德国政府就把那些标记抹去，于是岛民又幸福地过上自己富有的生活。

读到这里读者朋友也许会发出这样的感慨：天底下竟存在这样荒唐的货币！但事实上，被视为现代经济学皇冠上最璀璨宝石的信用货币，其运行原理与雅浦岛石币并无不同。

（二）法兰西银行的黄金

弗里德曼在《货币的祸害》一书里举了一个例子：1932年，法兰西银行害怕美国不再盯住金本位，不再按一盎司黄金兑换20.67美元的传统价格兑换黄金。于是，法兰西银行要求纽约联邦储备银行将它存在美国的大部分美元资产转换成黄金。为了降低将黄金装船海运的成本，法兰西银行要求联邦储备银行把黄金存到法兰西银行的会计账簿上。

于是财经报纸用头条报道了这条关于“黄金的损失”以及对美国金融体系的威胁等诸如此类的消息。美国的黄金储备开始减少，法国的黄金储备开始增加。市场认为美元走软，法郎走强。这种因法国向美国兑换黄金而造成的所谓黄金流失，甚至引发了1933年的银行业恐慌。

而事实上，黄金并没有流到法国，仍然在美联储的地下金库里，因为这只是一次会计操作而已。当时的实际情形是美国联邦储备银行在地下金库的抽屉上作了一些标记，表示这些抽屉中的金块属于法国了。

看起来雅浦岛的石币像是远古的实物货币，如法国人的兽皮，蒙古人的砖茶，印度原始居民的杏仁，中国夏代的海贝.....但是，雅浦岛居民的交易并不真正需要挪动或分割那些石币，他们只需要更改石币上的标记，甚至连标记也不需要。如果大伙脑海里有关于某一石币的共同记忆，那么大伙也都承认这笔财富的存在。

对，货币只是一种记账方式。不仅雅浦岛居民这样认为，美国联邦储备银行也这样认为，比特币等区块链货币也是这样认为。当文克莱沃斯兄弟宣称他们拥有100000枚比特币，不是说在某银行的保险箱里，真的有100000枚比特币整整齐齐码在那儿，而是说比特币全网节点都承认有这些一笔比特币，且归属于文克莱沃斯兄弟的比特币地址。

（三）货币的本质

让我们回到货币的本质。假想我们处在一个没有货币的世界，比如同样也是在一个遗世独立的小岛上，与雅浦岛不同，这个小岛还没有诞生货币。岛上只有我和你，现在我们需要进行一笔交易。我想要你手里的鱼，你想要我手里的浆果。那么很简单，我们直接互相交换就可以了。但是如果我现在手里没有浆果，我的浆果得在秋天才能收获，可是我现在又很需要你手里的鱼。那么我们该怎么交易呢？好吧，鉴于岛上只有我们两个人，你决定相信我，我给你发出一个IOU（I owe you），即借据，约定到秋天浆果收获的时候我支付给你，现在我就可以获得我

所想要的鱼。我们引入资产负债表的概念，让这个故事更一目了然（表1-1）。

表1-1 基于直接互换的资产负债表

我		你	
资产	负债	资产	负债
+ 鱼	+ Δ IOU	- 鱼 + Δ IOU	

在资产负债表中，我的资产由于获得鱼而增加，同时负债也增加，即对你的债务凭证。而你的资产端则是将交易给我的商品转换成了对我的债务追偿权。

现在我们来个稍微复杂的例子。假设你我素昧平生，彼此都不信任，那这个时候我们该如何进行交易？假设我们都信任一个第三方，比如银行，银行也乐意充当我们的桥梁，那么交易见表1-2。

表1-2 基于第三方的资产负债表

我		银行		你	
资产	负债	资产	负债	资产	负债
+ 鱼	+ Δ IOU	+ Δ IOU	+ Δ M	- 鱼 + Δ M	

我把自己的IOU转换成向你所认可接受的第三方发出的IOU，在这里由银行发出的IOU即银行券（bank note）。这样如资产负债表所示，我在资产端获得所需商品，负债端为对银行的IOU；而银行的资产端则为我发出的IOU，在负债端银行以我发出的IOU转换为对你发出的银行券（钱）。你的资产就由商品转换为银行券。

所以在现代社会，货币就是一种特殊的IOU，无论把货币当作是贷款还是债务，货币的本质都是一种记账方式。

当交易的群体不只是两个人之间，而是扩大到社会中的每个成员，当我们进行这种时间上不匹配的交易时，我们每个人都发出自己的 IOU，那么这个系统就会变得极为复杂（图1-1）。因为没有都认可的第三方时，我们每个人的交易都要取决于是否相信其他人，这将使我们在交易中寸步难行。于是我们不得不依赖于银行这种所谓“可信第三方”，可问题并没有解决，而是转化为另一个问题：银行真的值得信任吗？

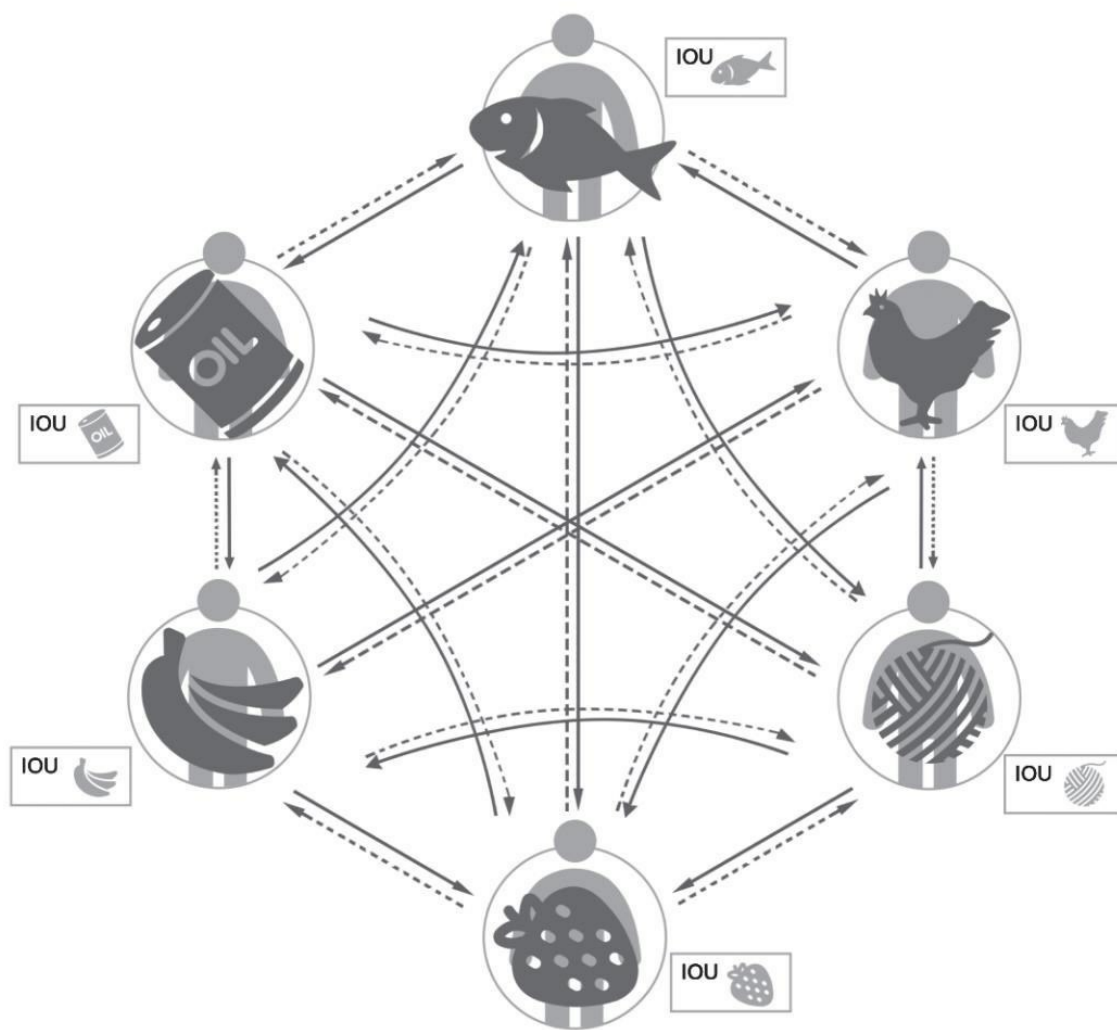


图1-1 无“可信第三方”的交换

（四）邓巴数限制

如果雅浦岛首富登上“非诚勿扰”，骄傲地宣称自己在太平洋底拥有一块非常值钱的石头，恐怕会被女嘉宾当成疯子羞辱。这种原始的货币制度只适合自然状态下的小规模经济，也就是费孝通在《江村经济》一书所说的熟人社会。雅浦岛石币无法突破邓巴数限制。人类学家罗宾·邓巴（Robin Dunbar）发现每个人与之维持持久关系的熟人，数量通常只有150个左右，这一数量限制就称作邓巴数。狩猎采集社会的典型组织单位“游团”的规模一般不足百人，比如非洲西南部卡拉哈里沙漠的桑

人，每个游团20~60人，邻近农耕区的游团100~150人；从事游耕农业的半定居社会，规模也只是略大，比如缅甸克钦邦山区的游耕群落，最大的也只有100多人。

雅浦岛之所以能孕育出如此神奇的货币现象，乃是因其处于自然经济状态，小岛居民人口不多，交易不普遍，货币的周转速度也非常慢。当地居民有的也许终其一生，也只有寥寥几次交易行为。幸亏雅浦岛上没有淘宝，没有电子商务，不然当地居民的脑子可能会“内存不足”。这也正是雅浦岛石币仅存于与世隔绝的大洋孤岛，而不见于人类主流社会的原因。

从地理上，没有比雅浦岛石币更孤独的了，它原产于西太平洋上的帕劳。但在理念上，它并不孤独，可以说它与比特币思想异曲同工。石币与比特币都具有稀缺性，前者是大自然的石灰岩矿藏分布，后者是基于数学算法；两者同样需要付出昂贵的劳力（计算力）成本才能获取，前者是冒险家的航海运输，后者是矿工的挖矿；两者交易总账均采用分布式存储，前者是大脑记忆，后者是计算机（表1-3）。幸亏有了计算机，人们终于不再需要用石头标记或集体记忆来记录交易，计算机网络可以帮助我们实现这一切。交易行为也同样打破了熟人社会的限制，在比特币交易过程中，交易双方不必彼此熟识或信任，也无须引入可信第三方，就能随时随地自由交易，也就是说，邓巴数被突破了。

表1-3 法币、石币、比特币特性对比

	各国法币	雅浦岛石币	比特币
稀缺性	基于货币政策	资源有限	总量有限，2100 万个
获取途径	中央银行发行	航海运输	哈希计算
交易方式	纸币/电子支付	修改标记/广播	网络节点的广播
交易总账	无/中心化银行	石头标记/大脑记忆	区块链
流通性	国家内部	孤岛	全球流通

（五）中心化缺陷

如果雅浦岛首富为富不仁，想要私下使用这笔巨款，比如偷偷跟自己的情人说我那块大石头送给你了，那么这次交易是无效的，因为交易没有广播，并没有其他岛民在旁边作证。但如果首富临死前，当着全岛人民的面说，这块大石头就作为遗产给我的大儿子了，那么这笔交易就是有效的，因为其他岛民都做了见证，并集体更新了头脑里的“账簿”。雅浦岛石币虽已具备分布式货币的雏形，但毕竟人肉信息传递网络是脆弱的，交易在口口相传的途径中以及集体记忆中极易出现差错。

比特币全网的节点每时每刻都在向网络广播交易，每笔交易经10~60秒就能广播至全球所有节点，速度取决于节点的网络连接状况。这些广播出来的交易在经过矿工的验证后，打包到数据块中，串联起来形成环环相扣的区块链，这些交易一经六次确认便几无篡改的可能性。要修改某个区块上的数据，得从这个区块开始重新计算之后的所有区块，考虑到比特币全网1300万亿次哈希运算的算力，地球上在比特币网络之外已不存在足以逆转比特币交易的计算能力。

雅浦岛的集体记忆式账簿虽然表面上是分散的，但仍然存在一个权威的第三方，可以决定石币的归属。然而在去中心化的区块链中，并无一个高高在上的殖民政府有权宣布没收你的比特币。或许从载体来说，石币是真实存在的实体，比特币只是虚无缥缈的数字，但从实用性来说，石币只是发人深省的寓言，比特币才是实实在在的财富。

数万年以来，雅浦岛岛民将他们在遥远的岛屿上开采出来，经过打制并运回自己居住岛屿的石头，充作交换的载体，他们一直这样独特地理解着金钱与财富；数千年以来，文明社会则把金块从地底深处开采出来，花大力气进行冶炼，经过长距离的转运，再次埋进精心设计的地下金库，金块的一举一动都可能引发金融市场的离奇波动；最近几年，矿工们满世界寻找着便宜的电力，大规模部署先进的ASIC芯片，挖掘一

种叫比特币的玩意，据说那是一串叫作Base58编码[\[10\]](#)的毫无意义的字符，居然能在全球100多家交易市场卖数百美元一个。听完上面这个故事，比特币是不是也变得不那么令人费解了呢？

三、信用篇

（一）库拉圈

社会学家马林诺夫斯基（Malinowski）考察完西太平洋上的特罗布里恩德群岛后，对古典经济学中的一个假设很生气。经济学家过去一直把人类视作“理性经济人”，假设他们在自由和竞争性的市场里同他人进行交易或交换时，总是寻求物质利益或效用的最大化。但特罗布里恩德群岛上的居民却不是这样。在他们的交易行为中，利益最大化似乎并不是他们考虑的首要前提。

在这些洋岛部落间存在着一种被称为库拉圈（Kula Ring）的封闭交换关系圈，当地居民生活的各方面都与库拉有着紧密的联系。库拉的核心是白色贝壳雕琢的臂镯和红色贝壳打造的项圈的交换，这种交易具有方向性，人们只能逆时针方向交换臂镯，顺时针方向交换项圈（图1-2）。

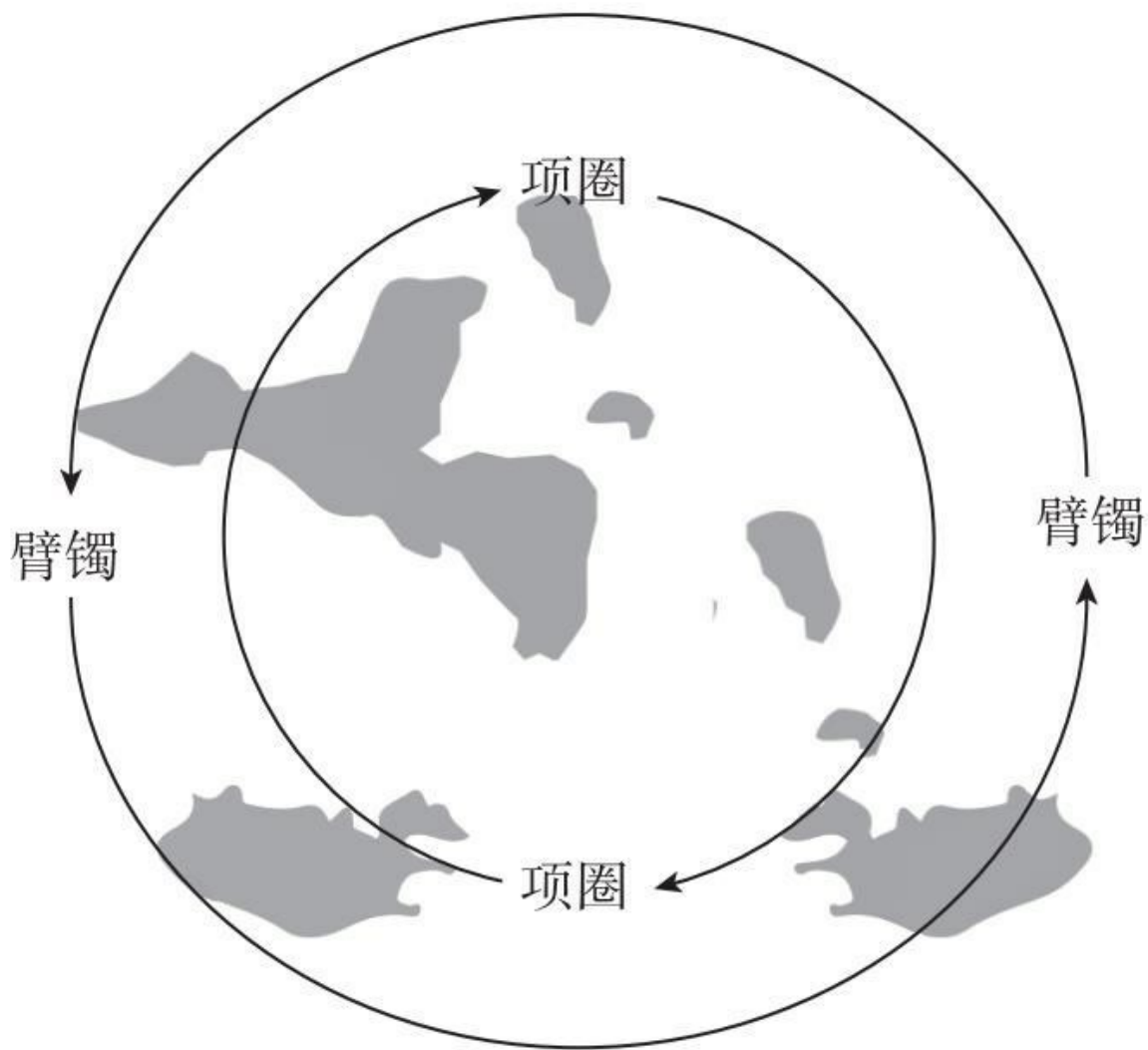


图1-2 库拉圈交换

库拉贸易圈大致覆盖了整个特罗布里恩德群岛。岛上的男人长途航行，横穿公海，按顺时针方向输运项圈；另一些人则按逆时针方向输运臂镯。一个人根据地位的不同，可能有一个到数十个的库拉伙伴。库拉伙伴是具有库拉关系的不同部落的土著。这是一种相对稳定的关系，关系一旦建立就基本不会被破坏。一旦进行库拉交易，则一直进行库拉交易，交易伙伴越多，他的部落地位越高。

当一个人从南方的库拉伙伴处得到臂镯，他会再把臂镯交换给处于北方的库拉伙伴。相反，当他从北方的库拉伙伴处得到项圈，会再次把

项圈交换给南方的库拉伙伴，从而形成按相反方向流动的两种库拉圈：臂镯以逆时针的方向流动，而相应地，项圈以顺时针的方向流动。处在库拉圈不同地方的土著基本按照这样的方式进行库拉。

马林诺夫斯基发现，库拉交易并不是等价交易，也不同时发生，而更像是一种礼物馈赠。一个人将臂镯交换给处于下游的库拉伙伴，上游的库拉伙伴一段时间后回赠项圈，臂镯和项圈的价值并不相等。如果臂镯的价值高，且人都是自私的话，那么他不应该将臂镯交换出去。但事实上，群岛上的每个库拉交易者都非常乐意将臂镯交换出去，而不是以占有为目的。正如马林诺夫斯基指出的：

“在特罗布里恩德岛民的库拉交换形式中甚至没有一丝要从中共获利的迹象，没有任何理由用纯功利主义的和经济的观点看待他们，因为他们没有通过交换而相互利用”。

（二）理性经济人

看到这里，读者朋友可能会觉得这群可爱的岛民都是乐施好善、淡泊名利的天使，但你要是了解他们种红薯的奇怪嗜好就不会这样认为了。特罗布里恩德人喜欢种红薯但他们并不吃红薯，因为岛上遍布野生的热带奇珍异果，既好吃又管饱，在这儿，农业更像是一种娱乐活动。他们种红薯的唯一目的就是堆在院子里炫耀，攀比谁的红薯堆大，然后储藏起来让它们烂掉。看来特罗布里恩德人同文明世界里的“土豪”一样，都喜欢炫耀自己的财富，以种红薯这样不算浪漫的方式诠释着浪费。但在库拉交易中，他们却并不以拥有臂镯和项圈多为傲，相反，他们以频繁交易为荣。这种交易要经历航海的千辛万苦，没有带来丝毫财富上的回报，这似乎很矛盾。

按照经典经济学中“理性经济人”的概念，小岛原住民的一切行为都是出于自利的理性考虑，他们过着一种“算计的、冷酷的、自我中心主

义的、斤斤计较于效用的生活”。马林诺夫斯基严厉地批评了这些观点。他指出，“库拉交易绝非纯粹的商业性交易，它不是建立在对实际效用和利润得失的简单计算上”。[\[11\]](#)

对库拉交易行为的合理性解释很多，一种解释认为这就是礼物馈赠，因为库拉交易中隐含着一种互惠逻辑：赠予礼仪性的礼物以后，不论时间长短，总要报以差不多等值的答礼。结构主义大师列维·施特劳斯的舅舅莫斯还根据这个社会学案例写了本著名的《礼物》。另一种解释认为这是宗教仪式，因为某些库拉交易还伴随着精致的巫术仪式和公共仪礼。

但是，以上两种解释都无法回答以下几个问题：①库拉交易为何要规定方向？②为何交易对象越多，交易者的地位越高？③为何交易次数越多，交易者的地位越高？

（三）等价交易

当今电子支付是如此快捷高效，以至于人们会有这样的疑惑：既然PayPal（贝宝）、支付宝已经如此方便，我们还需要基于区块链的数字货币支付吗？

答案是肯定的。在一次支付宝处理的交易中，一个人的支出等于另一个人的收入，这是等价交易。问题在于，如果支出与收入是同一个人的两个账户，会发生什么？由于对支付宝而言，每一笔交易的边际成本都近乎于零，所以，如果一个人同时拥有两个账户，他在两个账户里反复进行转账交易，就会以非常低的成本制造出无数被支付宝视作洪水猛兽的刷信用行为。

淘宝网非常明智地给交易引入了评价，但是无论采用多么高明的机器算法与人工干预，都无法阻止刷客与差评师这两种职业的存在。前者假扮成买家，通过虚假交易，对卖家的商品刷好评以赚取卖家支付的佣

金；后者给网上卖家恶意差评，以勒索卖家提供相应的“赔偿”以获利。

淘宝网通过非常复杂的手段遏制刷信用行为：一方面使用机器算法对店铺进行排查，将出现异常情况（如交易过于频繁）的店铺进行上报；另一方面设有2000多人的团队，对涉嫌刷信用和好评的店铺进行清查，但是收效甚微。这不仅是淘宝网的难题，也是所有电子商务平台的阿喀琉斯之踵。只因它们对交易行为的处理都是一样的，即等价交易。

等价交易的观念伴随着可切割熔铸的金属货币的使用而被人们广泛接受，并随着时间的推移而根深蒂固。公元前7世纪吕底亚人使用条状的金属或者扁豆状的金属块进行支付，可以精确地衡量商品的价值。王国的统治者克里萨斯国王因发达的铸币业而富有得令人难以置信，并因此就有了“像克里萨斯一样富有”的说法。

互联网电子支付对交易的处理与吕底亚人并无不同，只不过，PayPal、支付宝不再使用粒度不同的金属，而是使用服务器里妥善存储的数据。等价交易无须精确称量，而只需进行一次数据库操作。用户用电子支付的A账户给B账户转账金额为 m ，反过来，再从B账户转账金额 m 到A账户，电子支付数据库里A账户与B账户的数值又恢复到起始，如此进行无数遍，便是典型的刷信用行为。库拉圈交易也是一次循环（库拉的含义就是循环），不同的是库拉的交易有方向性，而不能作对换交易。

试想在特罗布里恩德群岛的库拉圈贸易中，若是一个人从南方的库拉伙伴处得到臂镯，不再把臂镯交换给北方的库拉伙伴（逆时针），也不把自己的项圈回赠给南方的库拉伙伴（顺时针），而是再次把臂镯还给这位南方的库拉伙伴，将意味着什么？没错，这是一次典型的刷信用式的死循环，臂镯将永远在这两位库拉伙伴中循环，而成为两人永久占有的私藏。两人在部落中也将“刷出”非常显赫的地位。显然，如果大家都这么投机取巧，那么所有的臂镯与项圈都将退出流转，变成藏而不露的私有财产，库拉贸易圈也将不复存在，而这正是库拉贸易要规定交易

的方向的缘故。交易一旦启动，库拉就会像接力游戏一样，一直按顺时针或逆时针方向流转下去。

库拉圈带给我们的启示是：如果规定交易的方向，就可以避免刷信用的行为。然而，这在真实经济中是不现实的，我们无法规定在电子商务中只允许与固定的人群交易，人们也的确有与自己交易的自由。

（四）将币天销毁引入信用评价

币天（CoinDays）销毁是区块链的一个非常重要的概念。顾名思义，币天销毁等于每笔交易的金额（币）乘以这笔交易的币在账上留存的时间（天），比如你花了一笔100天以前收到的10比特币，这笔交易的币天销毁就是1000币天。

起初，区块链研究者并没有注意到币天销毁的意义所在，因为它不像时间戳、难度、随机数等字段一样，在区块链中有明确的作用。只有少数对币价敏感的人群关注这个指标，他们认为区块链的币天销毁累积的变动，可以揭示市场走向。在市场处于下跌通道时，币天销毁的峰值意味着市场中的弱手，因为代表着大户可能要抛币。当市场处于上涨通道时，币天销毁的峰值意味着市场中的强手，表明市场可能会走强。与传统股票市场不同，在比特币等数字货币交易市场中，币天销毁比每日交易量这个指标更能准确地显示市场的资金流动。因为如果一个人开两个账户（比特币地址），用100个比特币来回转账，这样可以把交易量做到很大，但币天销毁却几乎维持不变。

币天销毁第二次被引起重视是在权益证明（PoS）中。点点币创始人萨尼·肯为避免工作量证明机制（PoW）的算力浪费，设计了权益证明的共识方案：当创建一个权益证明的区块时，矿工需要创建一个“币权”交易，交易会按设定的比例把一些币发送给矿工本身，其原理与比特币的区块产出25个新币相似，不同的是其难度与交易输入的“币天”成反比，而与哈希计算力无关。由于权益证明的哈希运算只是基于时间与

已知数据，因此无法通过改进芯片性能来加快其运算速度。每一秒钟，每个点点币交易输出都有一定概率产生与其币天成正比的工作量[12]。显然，在权益证明中引入币天的初衷是防止矿工重复使用自己的币，因为如果挖矿难度仅与矿工的权益（拥有的币）相关，那么，每个币都可以成为“模拟矿机”，那些拥有大量币的人躺着就能挣钱（挖矿），持币较少的用户则只能喝西北风，而这正是权益证明饱受诟病的原因。但若挖矿难度是币天的函数，虽然这种“模拟矿机”的算力会随着时间累积而线性增长，但每发现一个新的区块其算力就随币天的销毁而归零，故币天可以保障权益证明机制中所有挖矿者的公平性。

以上两个应用实例虽然解决的是不同的问题，但本质上都是利用币天销毁在交易过程中不可逆的特性，使得用户不能在两个账户间反复利用同一笔钱获得某种回报。在市场中，大户不能利用同一笔比特币制造大量币天销毁虚构币的流动，在PoS挖矿中，用户不能利用同一笔点点币反复挖得区块中的新币。相应地，如果把币天销毁引入交易的信用评价呢？如果说币天销毁在市场预测与权益证明中的应用是小试牛刀的话，那么，它在信用评价中的作用则是锋芒毕露了。让我们看看为什么刷客与差评师们在区块链的信用体系中会混不下去。

如果规定把币天销毁作为信用评价因子，在一次交易中，销毁的币天越多，则信用评价的权重越高。当刷客试图给用两个账户反复交易而刷好评时，第一次交易的评价是有效的，但历史上累积的币天在交易完成之时便已销毁，当进行第二笔交易时，由于发生在第一次交易后不久，币天积累非常小。相应地，对信用评价的贡献微乎其微，其后所有交易的币天销毁之和同样也非常小，用户利用同一笔钱反复给自己刷好评，不管进行多少次，其最终效果与第一笔交易所带来的信用评价几乎一样。同样，当差评师试图通过大量小额交易给用户以恶意差评时，由于信用评价正比于币天销毁，交易的额度太小，同样也几乎不能对用户的信用产生影响。

也许在不远的将来，在淘宝、京东等电商平台泛滥成灾的刷客与差评师将会失业。需要指出的是，人们过去总是把信用当作一个道德问题，试图从道德层面约束交易行为。淘宝极其复杂的信用体系试图区分真实的交易行为与作弊交易行为，并通过大数据分析，结合用户的社会关系、职业、收入甚至公共事业缴费单，评价一个人的信用高低。然而在区块链的信用评价中，信用其实是一个数学问题。在刚才的例子中我们看到，用户的交易行为不再被区分为作弊交易与真实交易，而对所有的交易行为一视同仁，通过数学赋予交易以成本（币天销毁），便可以使信用评价结果准确地反映用户的真实信用。作弊是允许的，不存在一个中心化权威可以跳出来宣布冻结你的账户，但即使你作弊，也不会对任何人的信用产生影响。

（五）交易的热力学第二定律

目前第三方支付都把交易处理成等价交易，在一次交易中，一方的支出等于另一方的收入（式1-1）。这本身并没有错，只是还不够。在交易的过程中，还需要引入时间之矢，用于区分一笔从A账户到B账户的交易与B账户到A账户的交易，虽然金额同样为m，但两个过程中销毁的币天不一样。

$$Q = \Delta U + W \quad (\text{热力学第一定律, } Q \text{ 为与环境交换的热, } \Delta U \text{ 为系统内能变化, } W \text{ 为与环境交换的功}) \quad (\text{式 1-2})$$

等价交易是个等式，而信用评价是个不等式。在交易的过程中，既包含交易金额的转移，又包含交易双方相互的评价。如果说等价交易就像是交易的热力学第一定律（式1-2），那么基于币天销毁的信用评价就好比发现了交易的热力学第二定律（式1-3）。

$V = V_a + V_b$ (V 为系统总财富, V_a 、 V_b 分别为 A、B 两人的财富值, 等价交换原理) (式 1-1)

$S_f > S_i$ (热力学第二定律, S_f 为系统最终熵, S_i 为系统初始熵) (式 1-3)

热力学第二定律讲的是在孤立系统内的不可逆过程, 系统的熵总是增加的, 也叫作熵增加原理。这一原理的克劳修斯表述是, 不可能把热量从低温物体传向高温物体而不引起其他变化。相似地, 我们可以得到热力学第二定律的交易式表述: 在交易过程中, 系统的币天总是销毁的, 不可能在一次交易中不销毁任何币天。

币天销毁的本质就是时间之矢。正如特罗布里恩德群岛的居民们规定了库拉交易的空间方向, 区块链上的交易则是用币天销毁标记了交易的时间方向。等价交易把交易理解为标量, 信用评价却把交易理解为矢量, 等价交易加上信用评价, 这才是交易的全部。

于是, 奇怪的库拉交易行为也可以进行解释了。原来, 岛民们并不是在做普通的等价交易, 而是在从事一个类似于信用评价的交易。一个人的交易伙伴、交易次数的多少决定了他的信用高低, 这确实符合信用的逻辑。信用也不取决于交易信物的价值, 占有库拉并不能提升个人财富, 相反, 还可能损害个人信用, 交易信物的价值很小, 交易行为本身才有价值, 库拉只有在流动中才能展现一个人的信用。那么, 岛民们不远万里地与库拉伙伴们交易, 也完全合乎他们的利益。虽说在院子里晒红薯堆的行为看起来简直“蠢萌蠢萌”, 但他们在交易库拉时却是不折不扣的精明人。库拉交易确实不是等价交易, 在这一点上, 马林诺夫斯基是对的, 但在岛民是不是“理性经济人”这个问题上, 他着实是错怪古典经济学家了。

最后问题来了：是谁设计了币天？如前所述，在区块链中币天并不是必须存在的字段，它可有可无。如果区块链是一部机器，那么从这部机器中去掉币天这个零件，丝毫不影响整部机器的运行。但事实上，从创世区块以来，币天就已经存在了。中本聪为什么添加币天这样一个字段，我们只能像Vitalik一样把这个归为碰巧吧。

四、区块链篇

（一）第五次计算范式创新

1970年是比特币的计时元年，比特币区块链的时间戳从1970年1月1日起开始计算秒数。

1970年，纽约清算所建立银行同业支付系统（CHIPS），以电子化的手段代替原来的纸质支付清算。当时采用的是联机作业方式，通过清算所的交换中心同9家银行的42台终端相连。

当然1970这个数字巧合并不是中本聪有意为之，区块链以1970作绝对时间的计算起点，是因为UNIX（尤尼斯）操作系统以1970年1月1日作为纪元时间，很多编程语言起源于UNIX系统，同时也在比特币代码中留下了历史的痕迹。20世纪70年代，采用UNIX操作系统的大型机大行于世，所以银行清算中心也因大型机的面世而步入电子化时代。这与其说是巧合，不如说是偶然中的必然。

分析现代社会进化过程的一种方法是观察计算范式，我们看到每隔10年就会有一次新的范式出现。20世纪70年代是大型机，20世纪80年代是个人电脑，互联网与移动互联网则是最近的两次范式创新，那么接下来10年呢？基于区块链加密协议的价值互联网很可能就是一种新的范式（图1-3）。

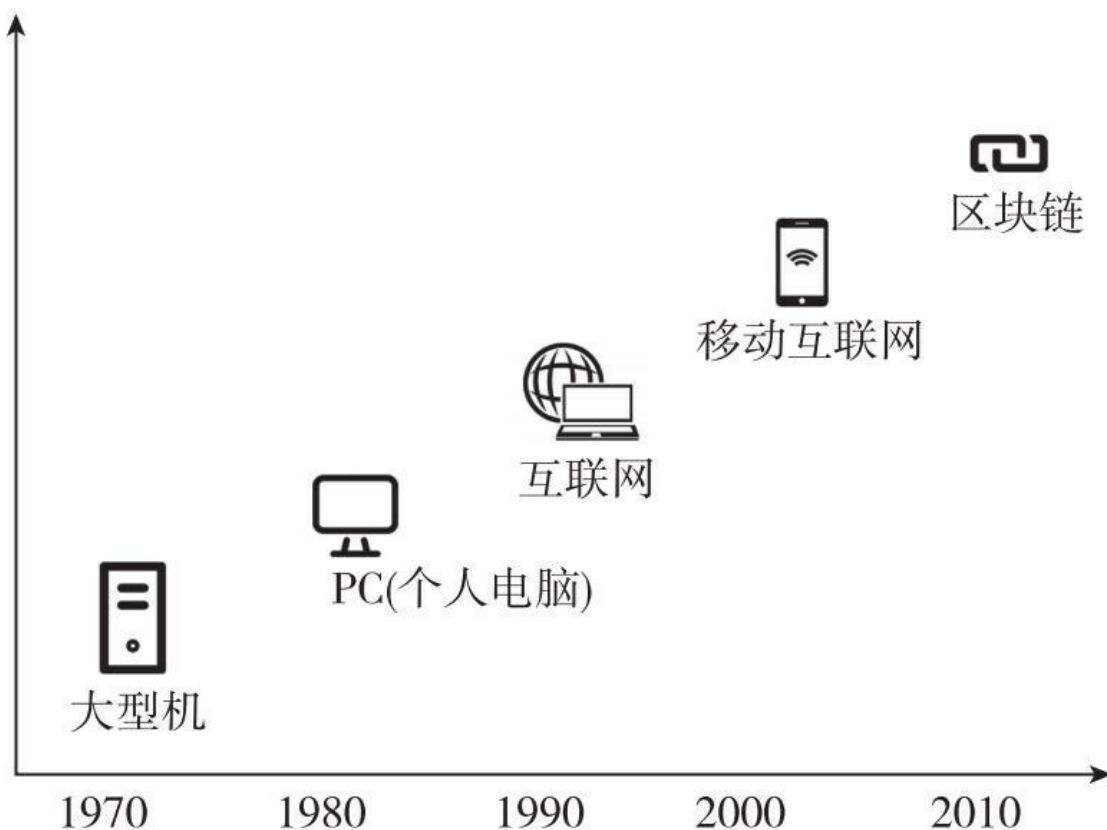


图1-3 五次计算范式创新

与声名大振的比特币相比，区块链技术一直默默无闻，但关于比特币的误解却一直影响着公众对区块链的认知，如与“丝绸之路”这样的网络黑市的种种关联，不免让人谈虎色变。事实上，各国政府部门、金融机构都在探索区块链技术的未来应用场景。它的以下四个特征，可能会给政府与金融服务带来跨越性创新^[13]。

1.通过加密技术对账

目前，政府和商业机构会把交易的详细信息发送给对方，一旦收到信息，每个机构都会在自己的账本上更新信息。但现在还没有一种方法可以保证这些信息的准确性。区块链可以通过分布式共识机制来解决这个问题。例如，通过工作量证明、权益证明等不同共识算法解决拜占庭将军问题，或通过“证据点”检验数据，账本的参与者就可以就底层数据

的状态达成共识。

2.数据复制

许多机构都有部分或全部数据的拷贝，这极大地降低了错误数据出现的可能性。对于现在的数据库技术来说，数据复制工作会增加IT（信息技术）系统的成本，并对IT系统的复杂性提出更高的要求。将数据大量复制的一个好处就是哪怕有一处数据出现错误，其他的数据还会是准确的。很多机构可以通过对账计算，检验其数据是否准确。

3.访问控制

分布式账本使用私钥和签名管理能够访问账本的权限。这些私钥在特定情况下具有特定的功能。举例来说，一名监管人员想检查一个机构所有的交易，可能需要一把“观察钥匙”，但这样的钥匙只有被法庭授权后才能具有这样的权限。

4.透明性和私密性

因为许多机构都拥有账本的备份，同时也可能验证每份记录的真伪，所以共享账本的透明性是很高的。因此，监管者或是独立第三方（司法）可以确信数据库的内容没有被篡改。鉴于此，他们可以公开原本是私密或不可公开的文件信息。在监管报告和欺诈预防方面，共享账本可以帮助银行等商业机构，甚至可以使民众拥有监督政府履行职责的能力。通过独特的数字签名技术，可以验证正确的人已经按照正确的规则添加了正确的记录。

（二）无银行间组织的跨行结算

生活中我们经常需要跨行、异地存取款，这会给银行之间带来高昂的结算成本。在没有银行间清算组织之前，需要解决两家银行之间的通

信问题。以图1-4为例，汇丰银行、花旗银行、渣打银行之间需要专门的通信接口，以满足双向通信的要求。

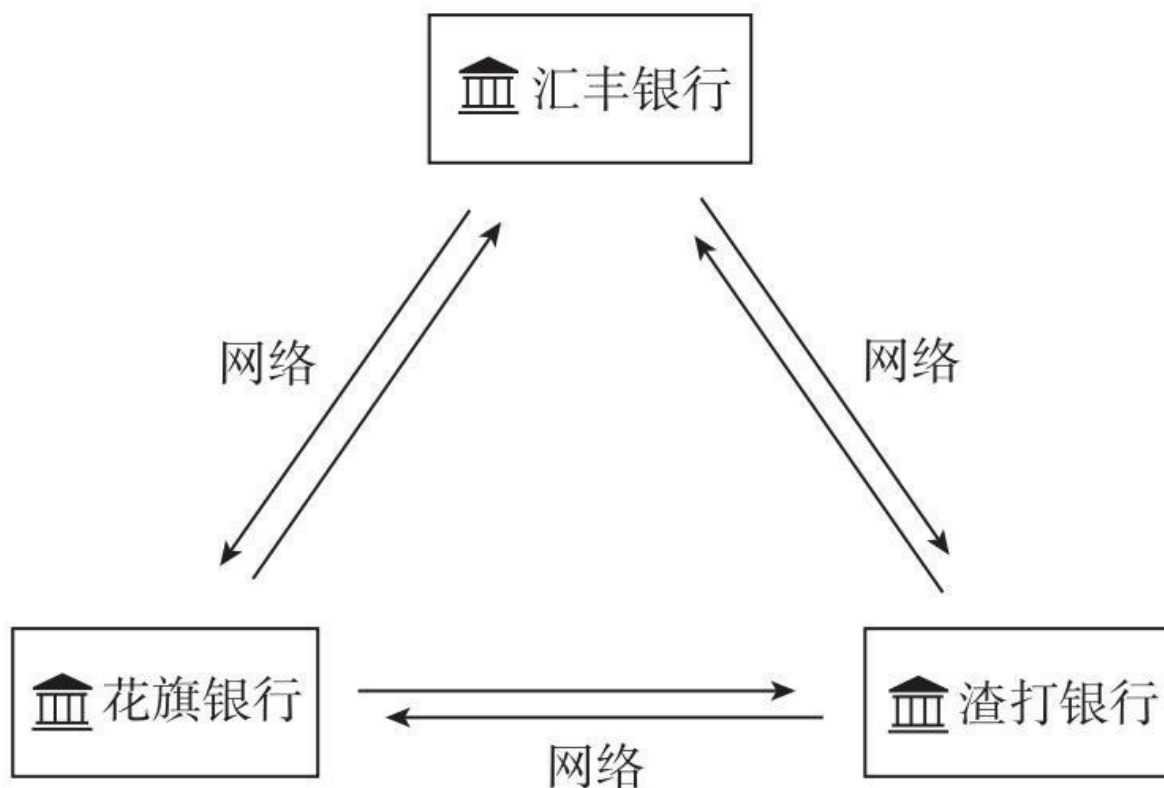


图1-4 无银行间清算组织的结算

下面，以银行的存付款为例，让我们设想有三个银行：汇丰银行、花旗银行、渣打银行；两个用户：用户A和用户B。每一个银行都有独立的信息系统，来核算自己的收支情况。汇丰银行的信息系统记录自己的客户的账户收支，花旗银行的信息系统记录自己的客户的账户收支，以此类推（图1-5）。

汇丰银行		
货币类型	交易者	交易金额
GBP(英镑)	花旗银行	1000000.00
GBP	渣打银行	5000000.00
GBP	用户	1000.00
GBP	用户	5000.00

花旗银行		
货币类型	交易者	交易金额
GBP	花旗银行	1000000.00
GBP	渣打银行	50000.00
GBP	用户A	500.00

渣打银行		
货币类型	交易者	交易金额
GBP	渣打银行	5000000.00
GBP	花旗银行	50000.00
USD(美元)	用户A	10000.00

用户A		
货币类型	交易者	交易金额
GBP	汇丰银行	1000.00
GBP	花旗银行	500.00
USD	渣打银行	10000.00

用户B		
货币类型	交易者	交易金额
GBP	汇丰银行	5000.00

图1-5 银行各自记录账户收支的信息模型

显而易见，我们可以发现两个问题。

第一，记录的重复性。看看银行的记账方式，汇丰银行的系统记录着“花旗银行欠汇丰银行100万欧元”，而花旗银行的系统也记录这个事务。也就是说，同样的事务被两个独立研发的系统记录了两次。而在其他领域，这种重复更加庞大也更加昂贵。

第二，记录者风险。看看用户A在汇丰银行和渣打银行有存款，而他在花旗银行是处于透支状态。也就是说，汇丰银行和渣打银行欠用户A钱，那么是谁记录这个欠钱的事务呢？汇丰银行和渣打银行自身！用户A不得不相信这两家银行会妥善处理自己放在银行的钱，银行会保持所有记录的准确性。我们习惯地将这种情况视为理所当然，但总感觉哪里不对劲吧。毕竟塞浦路斯银行危机这样的事就发生在不久前，如果有

一天，你拿张祖传的100万美元存单，银行说上面只有1000元.....

因此我们看到了两个有趣的现象：存款方不得不相信银行会妥善保管存款，并准确记录账户信息。而银行自己也不得不花费大量的时间和金钱来建立一套系统，以相信自己可以妥善保管用户的钱并保持账户信息的准确性。然后同业银行之间会花费更多的时间和金钱，互相检查，以保证它们的系统可以达成一致。

即便是在简单的模型里面，也至少有7处需要对账（图1-6）。银行里的“事务”通常最少要由两个不同的实体记录，并且需要昂贵的重复确认过程来保证各方的记录是一致的。

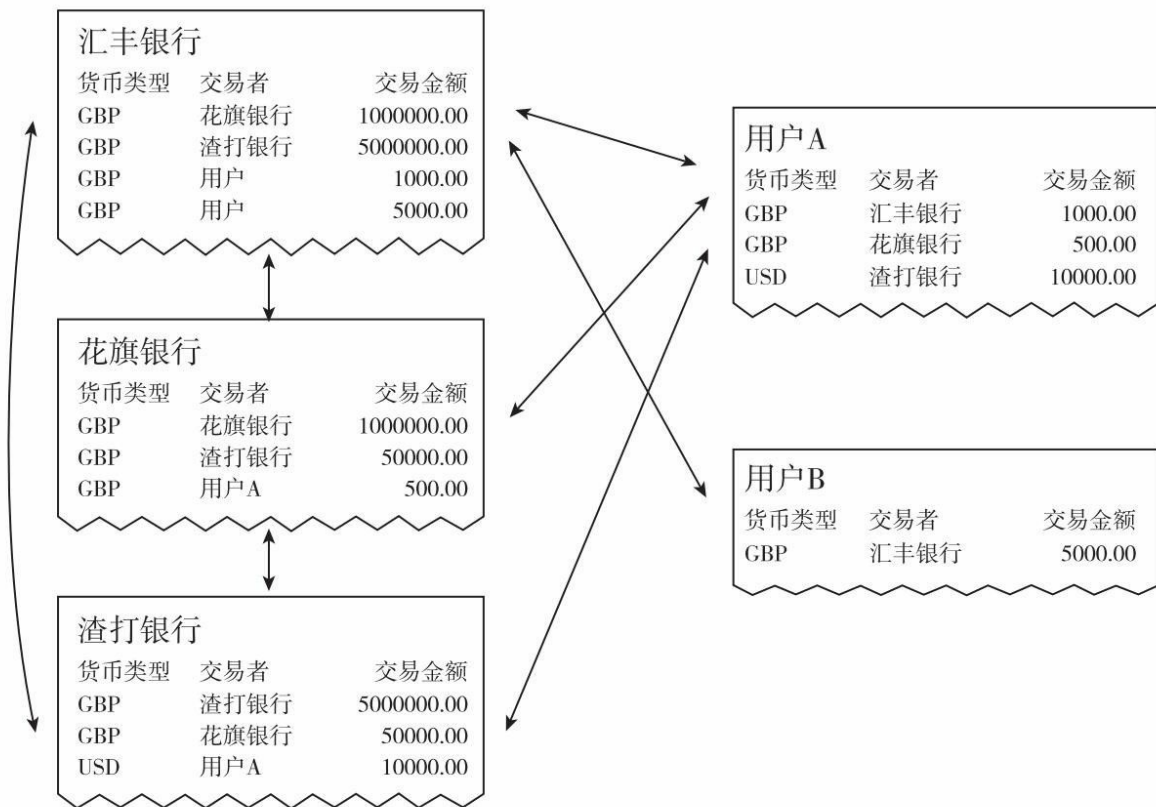


图1-6 对账的简单模型

在没有清算系统之前，同业银行之间的来往增多以后，会快速增加银行之间的清算网络 and 成本。这还只是三家银行的简单模型，通信网络就增加到6条，当银行越来越多的时候，这种点对点的通信变得越来越复杂，每新增一家银行，要做之前银行都要做的重复性工作，成本非常高昂。

如果一家银行与业内的1000家银行之间建立清算链接，该银行需要建设1998条通信链路。类似于足球比赛中主客场之间比赛，20支球队之间的联赛，每支球队需要参加38场比赛，30支球队的联赛每支球队需要踢58场比赛。

上述例子套在保险业和金融衍生品系统也是完全合适的。事实上对后者而言，这个模型带来的问题会更加严重，因为我们不仅仅需要确认

谁和谁做了什么样的交易，还要确认他们以及他们的系统都同意交易带来的结果——他们一定要在商业逻辑上达成一致。

想一想在金融领域有多少几乎一样的系统存在，每一个都几乎无差别的运行，制造更加几乎无差别的结果，这些结果不得不以昂贵的方式检查和解决，花费是十分巨大的。

（三）中心化的共享式总账

如果每一个银行都运行自己的系统，是如此昂贵和复杂，并且不可避免地带有局限性，不得不在与其他系统重叠的部分反复检查以互相匹配，那为什么不直接让大家使用，由大家都相信的某权威运行的一份统一单独的总账（如图1-7）？

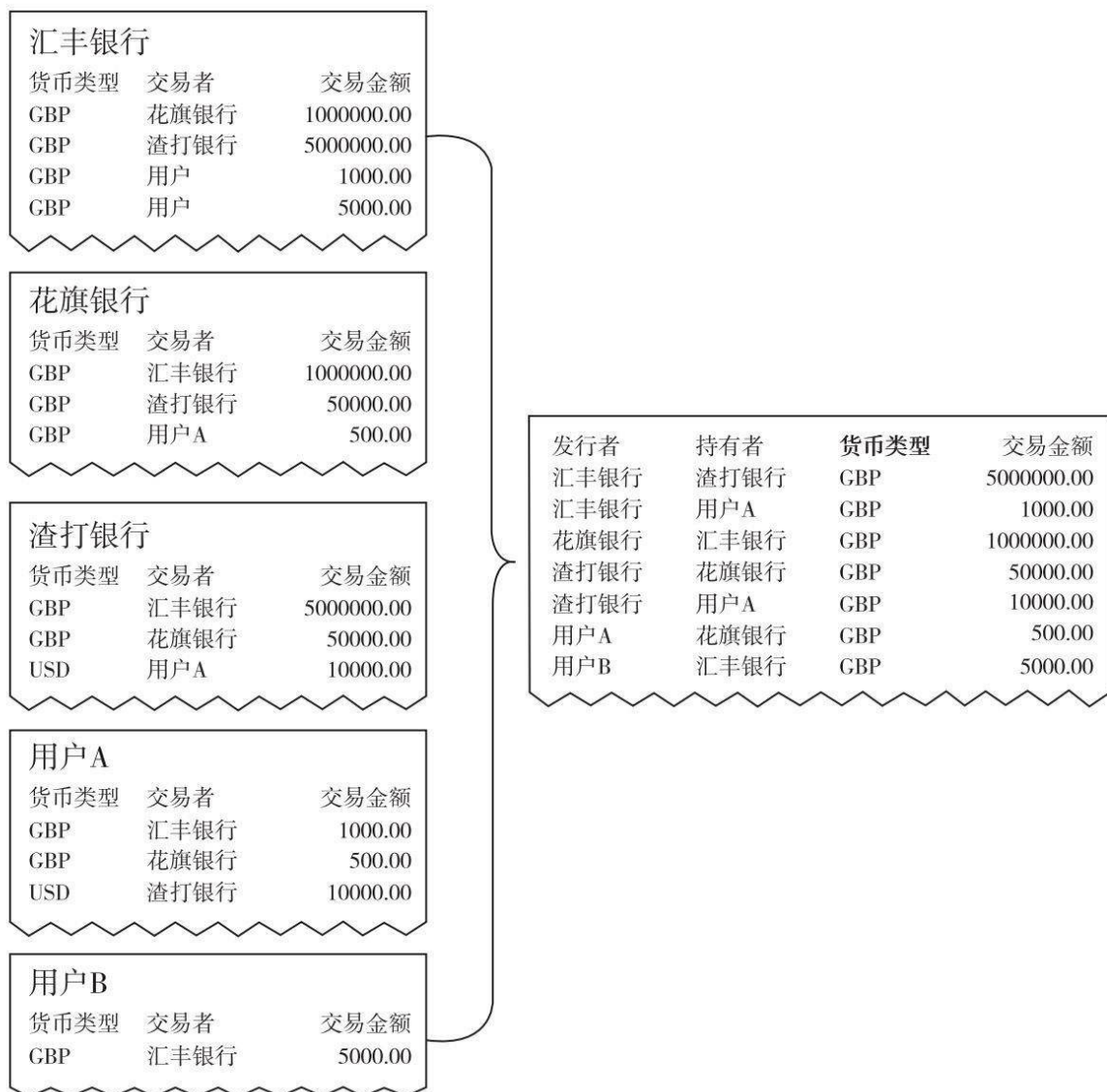


图1-7 中心化共享总账的对账模型

图1-7 左边的5张分开的表格合并后，可以完全等价地写成右边单一的表格，同样从右边的表格也很容易复原出左边的5张表格，唯一的不同是右边的表多一列。这样我们就可以用一张表记录一切，并且得到与原来的方案相同的结果。每个银行都可以毫不费力地从这个总账本中找出与自己相关的部分。

那么必须出现一个网络来保管右边这统一的表格，而且它能够接入所有的银行。新的银行只需接入这个网络，就可以和其他所有银行进行

通信，清算所和银行间组织就这样应运而生。

（四）有银行间组织的跨行结算

说起美国银行业清算系统的由来，还有一段趣闻。在两百多年前，两个银行职员의 偶遇擦出了债务交换的火花，成为现代银行间清算系统的雏形。那天，两个不同银行的职员在收账的路途中小憩，碰巧走进了同一家咖啡店。闲聊中，得知相互都要去对方那里取送票据，于是灵机一动，干脆在咖啡店进行交换算了，这样就可以省掉去对方营业地的旅途劳顿。从那以后，喝咖啡成了他们的正差，交换票据成了副业。如此滋润的事自然吸引了其他同行，他们纷纷加入进来，于是这家咖啡店变成了不叫清算所的清算所。

如果说咖啡店票据交换场所尚处于蹒跚学步阶段的话，那么1853年由62家银行在华尔街14号地下室共同创立的纽约清算所则标志着银行清算所已步入成年。**CHIPS**（纽约清算所银行同业支付系统）是全球最大的私营美元资金交换系统，平均每天清算和处理1.5万亿美元的美国境内和跨境支付业务。

美国不仅拥有全球最发达的银行清算系统，还拥有全球最发达的资本市场清算系统，也是全球最大的信用卡清算中心。**VISA**（维萨）和万事达两大国际信用卡组织均为位于美国纽约的摩根大通银行，同时也是自动清算所的成员，纽约也就成为全球信用卡的发源地和支付清算中心。

在**VISA**和万事达等这样的信用卡组织出现之前，跨行结算复杂度高，成本高，速度极慢。信用卡组织出现后，形成中心清算的模式，所有银行和该中心建立清算接口，所有跨行之间的交易都汇总到该清算中心。清算组织的出现提升了跨行清算的速度，并降低了清算的成本（图1-8）。

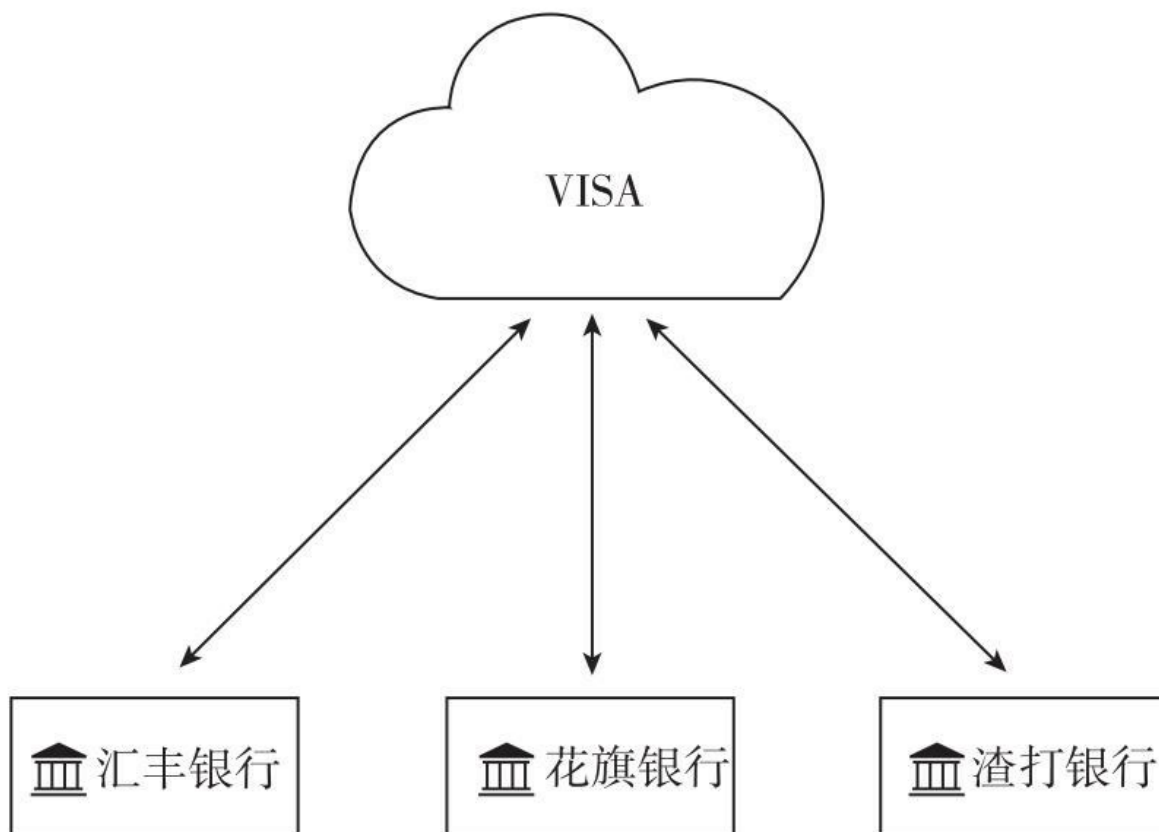


图1-8 有清算组织的银行间的跨行结算

但由于清算中心是中心化的架构，随着加入组织的银行成员增多，给清算中心带来收入的同时，也加大了工作量。在接入的银行超过一定程度后，再增加银行会员，就会显著增加清算中心的成本和工作量，从而降低清算速度。例如管理10人团队和管理10000人团队差别很大。目前，国际上三大信用卡上市公司VISA、万事达、美国运通2015年营业收入合计达到543亿美元。区块链技术实现分布式记账的结算之后，能为整个银行业节省一大笔费用。

清算、结算、托管和注册服务对于发行、交易和持有证券都会显著增加成本。有大量的专业代理和交易对手参与到投资者的证券和现金活动，不仅这些服务有特定的收费，还有处理各种不同系统接口的业务集成和流程的辅助成本。据估算，全球金融行业每年在交易后（post-trade）成本是650亿~800亿美元。图1-9以T+2交易机制为例，描述了主

流证券交易结算的多层次的复杂交易过程[14]。

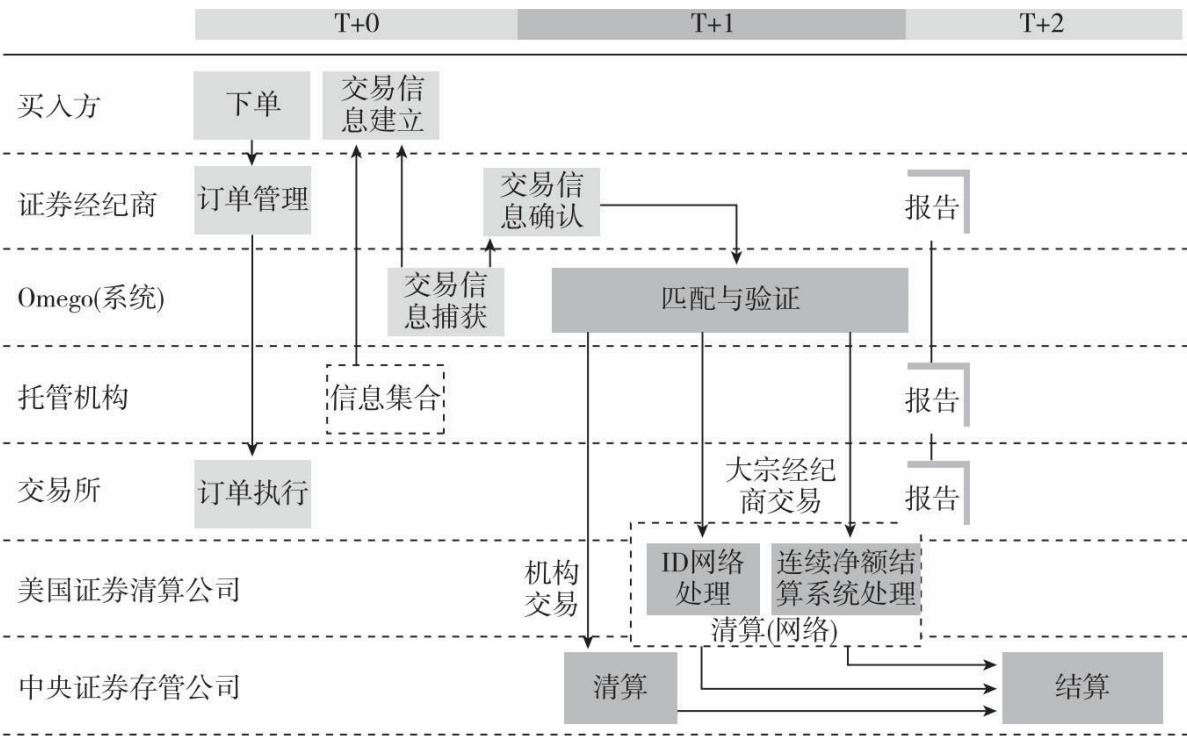


图1-9 美国证券交易的托管结算体系

同样，传统清算中心还面临中心化风险。例如“9·11”事件后，纽约联邦储备银行立刻停止靠近纽约的新泽西美元支付清算系统的运行，启动灾难备份系统，将美元支付清算系统从纽约新泽西切换到里士满和达拉斯。虽然在整个切换过程中，支付清算系统既没有中断服务，也没有丢失数据，但也惊出一身冷汗。如果袭击的不是世贸大楼，而是新泽西的美元支付清算系统，那么纽约清算中心将立即崩溃。

（五）去中心化的共享式总账

全球共享的账本可能被单一的强力实体控制，还有中心化的系统可能会有系统性的风险。因此我们可不可以对模型做两种微调？

第一，为什么不大量地复制账本，让每一个银行都保管一份拷贝？

这样，单点出现故障就不会影响总体，系统也会更安全，因为要篡改其中一份拷贝很容易，但要同时改动所有人的拷贝则很难。同样，每一个银行都有一份总账本拷贝也能使现存金融机构的整合变得更容易，这也能推动共享式总账的接受度。问题是怎样保证这么多份拷贝实现同步？

第二，为什么不让这个系统的参与者——不仅仅是银行，也许还包括银行的用户——一起参与进来维持和保护这个系统呢？毕竟，银行和用户都是这个系统的直接利益攸关方，不用怀疑他们任何一方保护自己的钱与监督对方的动力。任何一方欺骗都会被及时发现并受到惩罚。因此我们将一个单一权力的实体替换为每一个人都参与系统安全的新模型。

如果以上设想成立，账本看起来应该是这样的（图1-10）。

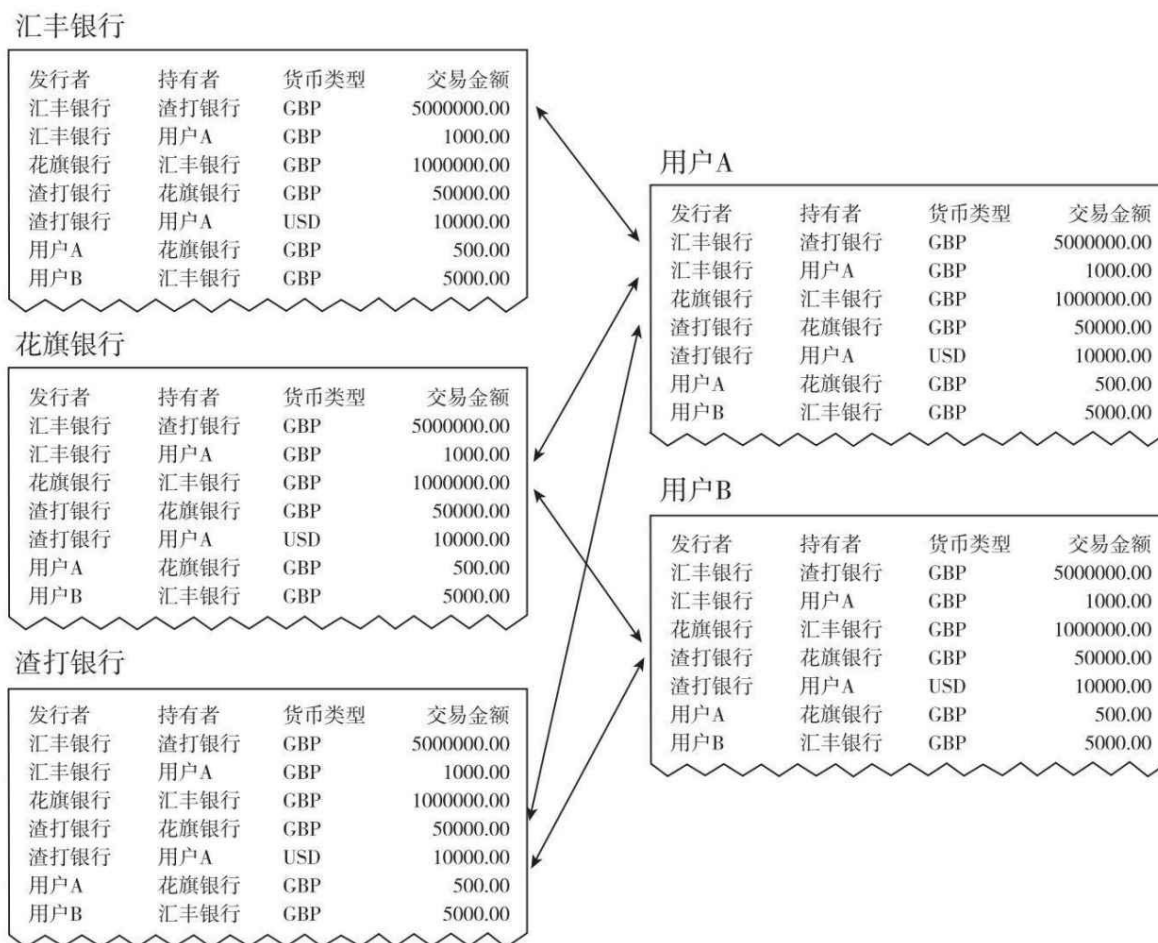


图1-10 银行与用户共同参与的系统模型

在这个模型中，所有的参与方都有一份总账的拷贝，但是只有修改自己部分的权限，因此它既是可复制的又是分布式的。

如果一个全球化的分享式总账存在风险，那么区块链就是对各方有利的最佳选择。区块链技术以点对点的方式运行一个分布式共享账本，参与者通过非对称加密的公私钥对执行交易，这显著降低了交易结算的复杂性和交易后的服务成本。

区块链几乎不存在单点故障，数据存储在全球数以万计的节点之上，分布式网络每时每刻都有大量节点频繁地加入或退出，但丝毫不影响全局结构的稳定性。

交易数据以区块的形式被打包到数据库，每一个区块都会由节点进行审查。如果所有节点达成共识，该区块包含有效交易时就会被添加到数据库中。此外，建立和维护这些节点是完全自治的，不需要也不允许任何一个控制或监管实体的存在。

由于区块链清算和结算几乎达到同步，系统在点对点网络上运行，每一笔交易都能确保准确执行，安全透明，每笔交易都能被网络上所有节点核实，而不是依靠一个中心化机构，因此其交易几乎不能被篡改。几乎所有无形的文件或资产都能以编码的形式表达，交易历史既可以被记录且公开，也可以被自主隐藏。隐私的选择权在于私钥的拥有者用户本人，使参与者能更自主地管理自己的隐私，监管者更有效地监管资产的流动。

[4] 本章由长铗完成。长铗,巴比特 (www.8btc.com) 创始人, 区块链研究者, 科幻作家, 2006~2008年连续三届中国科幻小说最高奖银河奖得主。合著有《比特币——一个真实而虚幻的金融世界》(中信出版社), 合编有《2014~2015中国数字货币行业发展研究报告》(上海社科院出版社)。巴比特创立于2011年, 专注于区块链资讯、数据、社区与区块链众筹服务, 现已发展为国内入口级区块链基础信息与数据服务平台。

[5] Dominic Frisby.搜寻中本聪.巴比特, 2014.

[6] 由罗纳德·维斯特、阿迪·萨莫尔和伦纳德·阿德曼三人姓首字母为名的一种加密算法。

[7] Napster是一款可以在网络中下载自己想要的MP3文件的软件。

[8] 维基解密创始人朱利安·阿桑奇也是密码邮件组成员。

[9] 解密学家猜测中本聪可能是英国人, 或受到英国文化影响, 这不无道理, 因为大多数人可能都会采用damn hard (非常地困难) 或者更简单粗暴的语言。

[10] Base58是比特币中使用的一种独特的编码方式, 主要用于产生比特币的钱包地址和私钥。

[11] 马林诺夫斯基.西太平洋的航海者.梁永佳, 等, 译. 北京: 华夏出版社, 2002.

[12] Vitalik Buterin.什么是权益证明以及为什么它重要.巴比特, 2013.

[13] 英国政府首席科学顾问报告《分布式账本技术: 超越区块链》。

[14] DTCC: 拥抱颠覆者——探索分布式总账技术潜力, 改进交易后场景。

第二章

区块链基础^[15]

一、区块链的基本概念

区块链（Blockchain）技术的产生和发展离不开比特币。首先，因为随着比特币的诞生，区块链技术才得以公布于众；其次，比特币是截至目前区块链技术最成功、最成熟的应用案例。比特币的概念由中本聪在2008年发表的论文《比特币：一种点对点的电子现金系统》中首次提出。文中，中本聪将区块链技术作为构建比特币数据结构及交易体系的基础技术，将比特币打造为一种数字货币和在线支付系统，利用加密技术实现资金转移，而不再依赖于中央银行。比特币使用公钥地址发送和接收比特币，并进行交易记录，从而实现个人身份信息的匿名。交易确认的过程则需要用户贡献算力，共同对交易进行共识确认，从而将交易记录到全网公开账本中。用户可以利用电脑、手机等发送或接收比特币，并选择交易费用。现有逾百种加密数字货币（未来币、点点币、莱特币、狗狗币等），比特币约占所有加密数字货币市值的90%。

比特币的区块链毕竟是为比特币体系的设计而定制，因此比特币的区块链技术并不等于区块链技术。区块链技术应该是可以有更多种形态、更多种体系、更多种用途、更多种规格的技术，其概念为：区块链是一个去中心化的分布式数据库，该数据库由一串使用密码学方法产生的数据区块有序链接而成，区块中包含有一定时间内产生的无法被篡改的数据记录信息。

区块中包含数据记录、当前区块根哈希（Hash）、前一区块根哈

希、时间戳以及其他信息（图2-1）。数据记录的类型可以根据场景决定，比如资产交易记录、资产发行记录、清算记录、智能合约记录甚至物联网数据记录等。数据记录在存储过程中，通常组织为树形式，比如默克尔树，而区块根哈希实际就是数据记录树的根节点哈希，为根据数据记录树自下而上逐步通过SHA-256等哈希算法计算得出。时间戳为区块的生成时间。其他信息包括区块签名信息、随机值等信息，也可根据具体应用场景灵活定义。

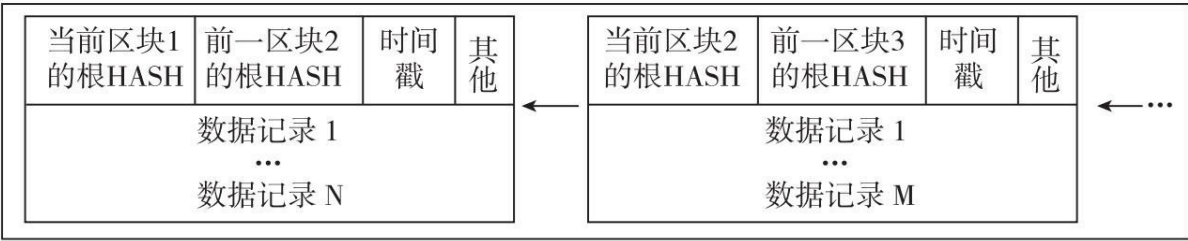


图2-1 区块链结构示意图

区块链技术不是一种单一的技术，而是多种技术整合的结果，包括密码学、数学、经济学、网络科学等。这些技术以特定方式组合在一起，形成了一种新的去中心化数据记录与存储体系，并给存储数据的区块打上时间戳使其形成一个连续的、前后关联的诚实数据记录存储结构，最终目的是建立一个保证诚实的数据系统，可将其称为能够保证系统诚实的分布式数据库。在这个系统中，只有系统本身是值得信任的，所以数据记录、存储与更新规则是为建立人们对区块链系统的信任而设计。诚实意味着系统可以被信任，正是商业活动和应用推广的前提，所以区块链技术已经被很多领域主流机构看中并非是没有理由的。因为有了区块链技术，在一个诚信的系统里，可以省去许多烦琐的审查手续，许多因数据缺乏透明度而无法开展的业务可以开展，甚至社会的自动化程度也将大幅提升。

近年来，包括高盛、摩根大通和纳斯达克等金融机构开始展开对区块链技术的重点研究。这些机构的金融业务大都具有标准化程度高、连

续性强、自动化需求大、业务对信用度要求高等特点，跟区块链的优势高度契合。同时，在供应链金融中，由于物流、资金流和信息流的复杂安排会涉及众多单据，因此使用电子商务平台记账会大大节省纸质单据所需要的时间和成本，然而使用谁的电子商务平台就成为一个大问题。如果使用利益相关各方自建的电子商务平台，数据的真实性就很容易受到质疑，而自建电子商务平台往往耗资不菲；如果使用第三方的电子商务平台，第三方的经营稳定性和信息安全性又难以保证，比如因财务、政策、网络攻击等各种情况引起不稳定问题等，沟通协调成本和风险也会大幅增加。区块链技术的安全性、不可逆、不可篡改性和透明性都已经得到了证明，如果能把供应链金融业务直接建立在这样已被证明其可靠性的区块链上，将极大地降低安全和信用成本。所以，尽管目前电子商务平台的使用已经大大节约了成本，但如果能有一个具有公信力的类似区块链公共信用系统，成本仍有进一步节约的空间。从政府层面来说，这一点也很重要，因为提供值得大众信任的系统本身就是政府职能的一部分。中国的资本运用效率远低于美国的一个非常重要的原因就是社会的信用体系不健全、信息不透明、部门协调成本过高，且利益保护现象严重。如果能从技术上应用区块链，就可以用较低的成本打破这些阻碍，建立一个公开的社会公共信用系统，整个社会成本都将大幅降低，效率也将大幅提升，还便于监管。透明的数据不仅将大大降低监管部门的工作量（很大一部分工作量转移给了社会监督，任何异动都很难逃过众人的眼睛），而且使得监管部门的主要工作转向治理，提升治理人性化和效率。

尽管使用区块链技术所建立的系统本身是诚实可信的，但这并不意味着来自系统以外的输入信息就是诚实的，更多的时候只是意味着区块链诚实记录并储存了这些外部数据。比如认证，认证工作往往是在线下完成，即使区块链能够存储文字、图片甚至多媒体信息，也并不意味着那些信息都是真实的。这并不意味着区块链真实记录并存储了这些信息，防止被篡改，如果发生业务纠纷时可以作为凭证。可能许多人没有注意到这一点，自动化是区块链技术的一个非常重要的特性，区块链网络实

际上就是一个接近于自动化或存在完全自动化可能性的网络。这一点之所以重要，一方面，是因为自动化是金融机构青睐区块链技术的重要原因，金融交易需要网络能够自动记录和存储交易数据，也能够允许参与者通过设置条件在网络上自动进行和完成交易；另一方面，区块链技术在这方面提供的可能性为社会生产效率的大幅提升留下了广阔的空间，也为智能合约等一系列高级应用留下了充足的余地。在理想情况下，区块链技术最终能够同物联网结合起来。

总体而言，区块链的发展体系可以划分为四个象限（图2-2）。第一象限是比特币区块链；

第二象限是使用比特币区块链协议，但不使用比特币货币的系统，比如万事达币、彩色币、合约币，以及采用合并挖矿的域名币等；第三象限是同时使用独立货币和独立区块链的系统，比如以太坊、瑞波、莱特币和未来币等；第四象限是侧链，采用独立的网络但以比特币作为底层货币的系统，如BTC Relay等。

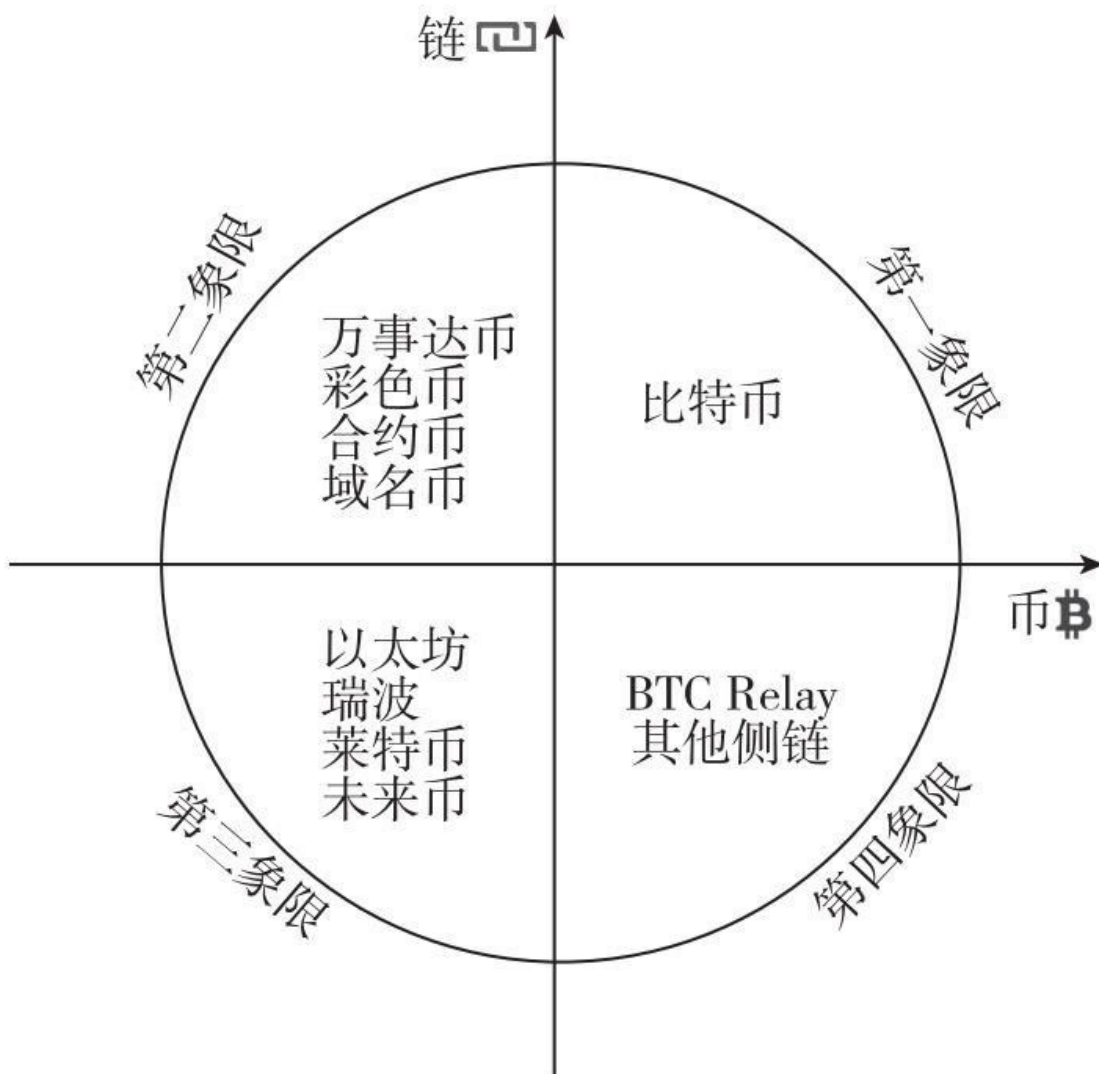


图2-2 区块链发展体系四象限

(一) 区块链的分类

目前已知的区块链技术应用大致分为三类。

1.公共区块链（Public Blockchain）：是指全世界任何人都可读取、可发送交易进行有效性确认，任何人都能参与其共识过程的区块链（共识过程是维持区块链这种分布式数据库一致性、准确性的关键技术，将在后续章节详细介绍），如图2-3所示。区块链上的数据记录公开，所有人都可以访问，都可以发出交易请求，并通过验证被写入区块链。共

识过程的参与者通过密码学技术共同维护公共区块链数据的安全、透明、不可篡改。公共区块链的典型应用包括比特币、以太坊等。

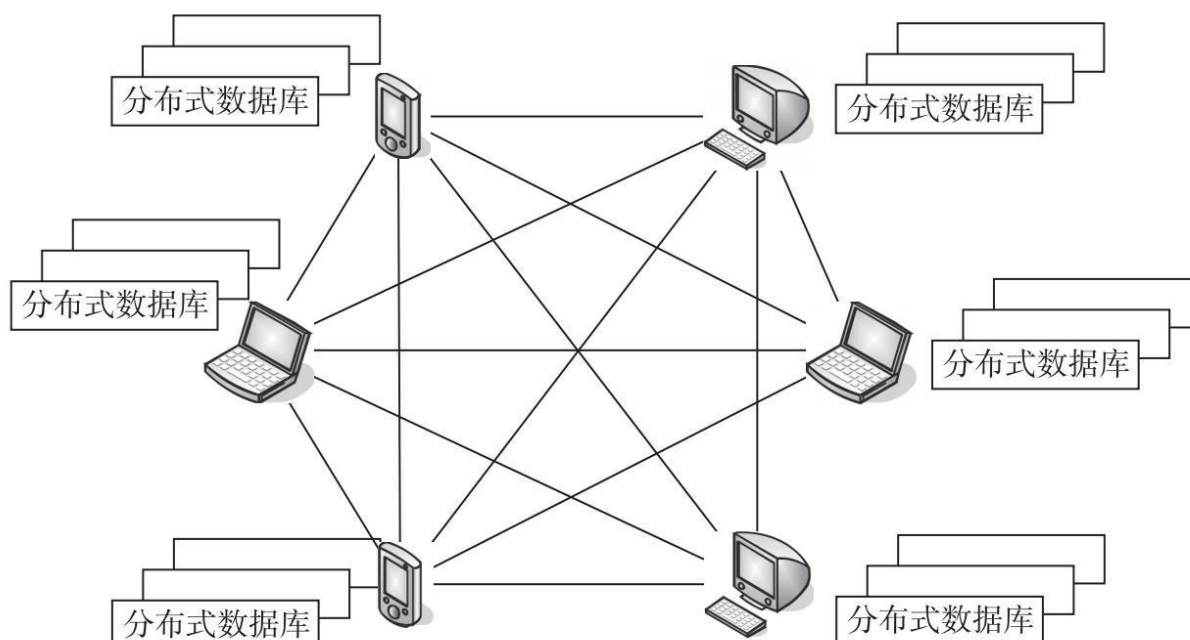


图2-3 公共区块链示意图

公共区块链是完全分布式的区块链，区块链数据公开，用户参与程度高，同时易于产生网络效应，便于应用推广。然而，系统的运行需要依赖于内建的激励机制。公共区块链上试图保存的数据越有价值，越要审视其安全性以及安全性带来的交易成本、系统可扩展性问题。

2.共同体区块链（Consortium Blockchains）：又称联盟链，是指参与区块链的节点是事先选择好的，节点间通常有良好的网络连接等合作关系，区块链上的数据可以是公开的也可以是内部的，为部分意义上的分布式，可视为“部分去中心化”。如图2-4所示为共同体区块链示意图。比如有若干家金融机构之间建立了某个共同体区块链，每个机构都运行着一个节点，而且为了使每个区块生效需要获得至少其中10个机构的确认。区块链可以允许每个机构可读取，或者只受限于共识验证参与者，或走混合型路线，例如区块的根哈希及应用程序接口对外公开，允

许外界用来进行区块链数据和区块链状态信息查询等。其典型应用包括超级账本（Hyperledger）、区块链联盟R3CEV等。

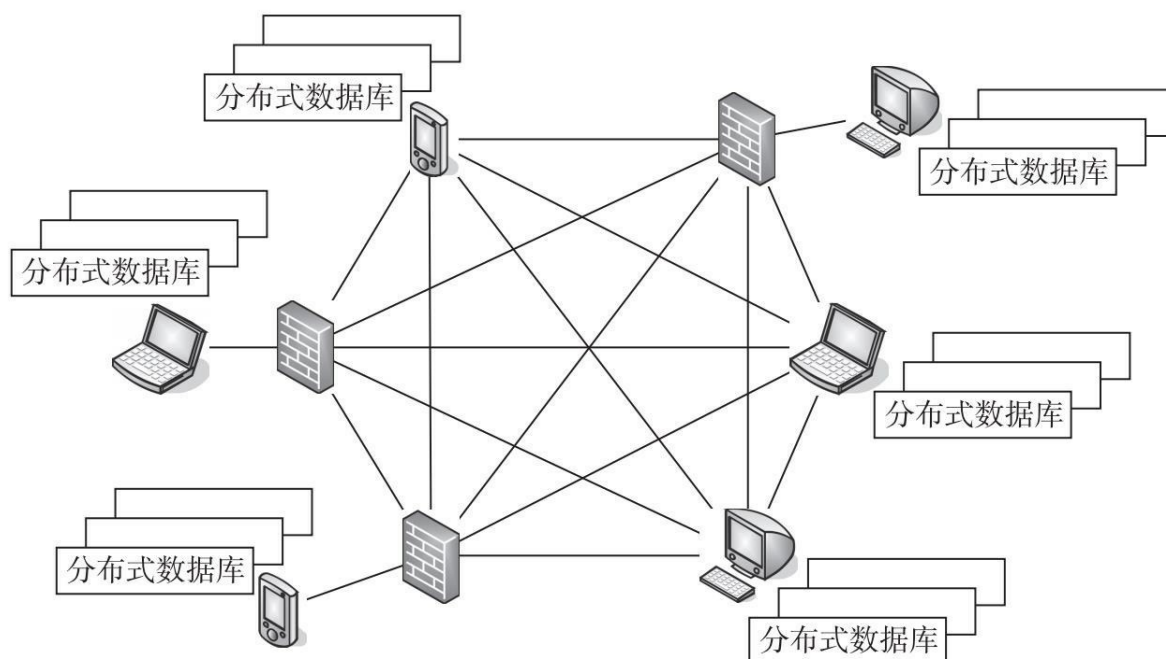


图2-4 共同体区块链示意图

共同体区块链的参与节点间的连接状态较好、验证效率较高，只需较低的成本即可维持运行，提供高速交易处理的同时降低交易费用，有很好的扩展性，数据可以保持一定的隐私性。但是这也意味着在共识达成的前提下，参与节点可以一起篡改数据。

3.私有区块链（Private Blockchain）：参与的节点只有有限的范围，比如特定机构的自身用户等，数据的访问及使用有严格的权限管理，如图2-5所示为私有区块链示意图。完全私有的区块链中写入权限仅在参与者手里，读取权限可以对外开放，也可以进行任意程度的限制。相关的应用囊括数据库管理、数据库审计甚至公司管理，尽管在有些情况下希望私有区块链可以具有公共的可审计性，但在更多的情况下，没有公共的可读性。由于是私有用户说了算，里面的数据没有无法篡改的特性，对于第三方的保障力度大大降低。因此，目前很多私有区

区块链会通过依附在比特币等已有区块链的方式存在，定期将系统快照数据记录到比特币等系统中。其典型应用如Eris Industries。

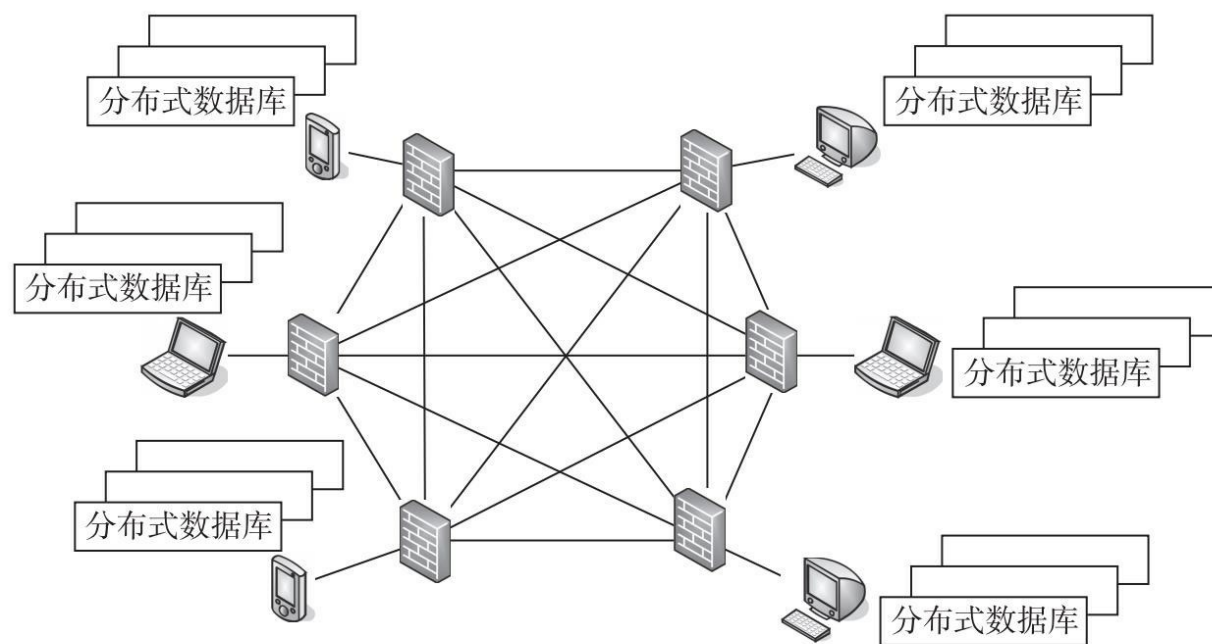


图2-5 私有区块链示意图

私有区块链可以带来规则的改变。如果需要的话，运行着私有区块链的机构可以很容易地修改区块链的规则、回滚交易。这一点似乎略有违背区块链的本质，但是却适用于一些特殊场景需求。由于私有区块链验证者是内部公开的，所以并不存在部分验证节点共谋进行51%攻击的风险。私有区块链交易成本更低。交易只需被几个受信的高算力节点验证即可，而不是需要数万个节点的确认，因此交易成本会低。但从长远来看，随着区块链技术的进步，公共区块链的成本将可能降低1~2个数量级，大致与高效的私有区块链系统类似。私有区块链节点间连接情况好、故障可以迅速通过人工干预来修复，从而提升交易速度并可以更好地保护隐私。

公共区块链、共同体区块链和私有区块链各有优势。公共区块链很难实现得很完美，共同体区块链、私有区块链需要找到实际迫切需求的

应用需求和场景。至于具体选择哪套方案取决于具体需求，有时使用公共区块链会更好，但有时又需要一定的私有控制，适用于使用共同体区块链或私有区块链。

（二）区块链的特征

1.去中心化

去中心化是区块链最基本的特征，意味着区块链不再依赖于中央处理节点，实现了数据的分布式记录、存储和更新。由于使用分布式存储和算力，不存在中心化的硬件或管理机构，全网节点的权利和义务均等，系统中的数据本质是由全网节点共同维护的。由于每个区块链节点都必须遵循同一规则，而该规则基于密码算法而非信用，同时每次数据更新需要网络内其他用户的批准，所以不需要一套第三方中介结构或信任机构背书。在传统的中心化网络中，对一个中心节点实行攻击即可破坏整个系统，而在一个去中心化的区块链网络中，攻击单个节点无法控制或破坏整个网络，掌握网内超过51%的节点只是获得控制权的开始而已。

2.透明性

区块链系统的数据记录对全网节点是透明的，数据记录的更新操作对全网节点也是透明的，这是区块链系统值得信任的基础。由于区块链系统使用开源的程序、开放的规则和高参与度，区块链数据记录和运行规则可以被全网节点审查、追溯，具有很高的透明度。

3.开放性

区块链系统是开放的，除了数据直接相关各方的私有信息被加密外，区块链的数据对所有人公开（具有特殊权限要求的区块链系统除外）。任何人或参与节点都可以通过公开的接口查询区块链数据记录或

者开发相关应用，因此整个系统信息高度透明。

4.自治性

区块链采用基于协商一致的规范和协议，使整个系统中的所有节点能够在去信任的环境自由安全地交换数据、记录数据、更新数据，把对个人或机构的信任改成对体系的信任，任何人为的干预都将不起作用。

5.信息不可篡改

区块链系统的信息一旦经过验证并添加至区块链后，就会得到永久存储，无法更改（具备特殊更改需求的私有区块链等系统除外）。除非能够同时控制系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

6.匿名性

区块链技术解决了节点间信任的问题，因此数据交换甚至交易均可在匿名的情况下进行。由于节点之间的数据交换遵循固定且预知的算法，因而其数据交互是无须信任的，可以基于地址而非个人身份进行，因此交易双方无须通过公开身份的方式让对方产生信任。

二、区块链的工作原理

（一）拜占庭将军问题

拜占庭将军问题是容错计算中的一个老问题，由莱斯利·兰伯特（Leslie Lamport）等人在1982年提出。拜占庭帝国是5~15世纪的东罗马帝国，即现在的土耳其。拜占庭城邦拥有巨大的财富，使它的十个邻邦垂涎已久。但是拜占庭高墙耸立，固若金汤，没有一个单独的邻邦能

够成功入侵。任何单个城邦的入侵行动都会失败，而入侵者的军队也会被歼灭，使其自身反而容易遭到其他九个城邦的入侵。这十个邻邦之间也互相觊觎对方的财富并经常爆发战争。拜占庭的防御能力如此之强，十个邻邦中的至少一半同时进攻，才能攻破。也就是说，如果六个或者更多的邻邦一起进攻，就会成功并获得拜占庭的财富。然而，如果其中有一个或者更多邻邦发生背叛，答应一起入侵但在其他人进攻的时候又不干了，会导致只有五支或者更少的军队在同时进攻，那么所有的进攻军队都会被歼灭，并随后被其他邻邦所劫掠。因此，这是一个由不互相信任的各个邻邦构成的分布式网络，每一方都小心行事，因为稍有不慎，就会给自己带来灾难。为了获取拜占庭的巨额财富，这些邻邦分散在拜占庭的周围，依靠士兵相互通信来协商进攻目标及进攻时间。这些邻邦将军想要攻克拜占庭，都面临着一个困扰，也就是拜占庭将军问题。

邻邦将军不确定他们中是否有叛徒，叛徒可能擅自变更进攻意向或者进攻时间。在这种状态下，将军们能否找到一种分布式协议进行远程协商，进而赢取拜占庭城堡攻克战役的胜利呢？这就是拜占庭将军问题。

针对拜占庭将军问题的解决方法包括：口头协议算法、书面协议算法等^[16]。口头协议算法的核心思想如下：要求每个被发送的消息都能被正确投递，信息接收者知道消息的发送者身份，知道缺少的消息信息。采用口头协议算法，若叛徒数少于 $1/3$ ，则拜占庭将军问题可解。也就是说，若叛徒数为 m ，当将军总数 n 至少为 $3m+1$ 时，问题可解。然而，口头协议算法存在明显的缺点，那就是消息不能追根溯源。为解决该问题，提出了书面协议算法。该算法要求签名不可伪造，一旦被篡改即可发现，同时任何人都可以验证签名的可靠性。书面协议算法也不能完全解决拜占庭将军问题。因为该算法没有考虑信息传输时延、其签名体系难以实现且签名消息记录的保存难以摆脱中心化机构。

与已有方法相比，区块链技术将是更完美的解决方案。区块链是怎样来解决这个问题的呢？它为发送信息加入了成本，降低了信息传递的速率，并加入了一个随机数以保证在一段时间内只有一个矿工可以进行传播。它加入的成本就是“工作量”，区块链矿工必须完成一个随机哈希算法的计算工作量才能向各城邦传播消息。

当用户向网络输入一笔交易的时候，他们使用内嵌在客户端的标准公钥加密工具为这笔交易签名，这好比拜占庭将军问题中他们用来签名和验证消息时使用的“印章”。因此，哈希计算速率的限制，加上公钥加密，使一个不可信网络变成了一个可信的网络，使所有参与者可以在某些事情上达成一致。拜占庭将军问题的区块链解决方案可以推广到任何在分布式网络上缺乏信任的领域，比如说域名、投票选举或其他需要分布式协议的地方[\[17\]](#)。

（二）区块链工作流程

区块链的工作流程主要包括如下步骤（图2-6）。

- ①发送节点将新的数据记录向全网进行广播。
- ②接收节点对收到的数据记录信息进行检验，比如记录信息是否合法，通过检验后，数据记录将被纳入一个区块中。
- ③ 全网所有接收节点对区块执行共识算法（工作量证明、权益证明等）。
- ④区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是将该区块的随机散列值视为最新的区块散列值，新区块的制造将以该区块链为基础进行延长。

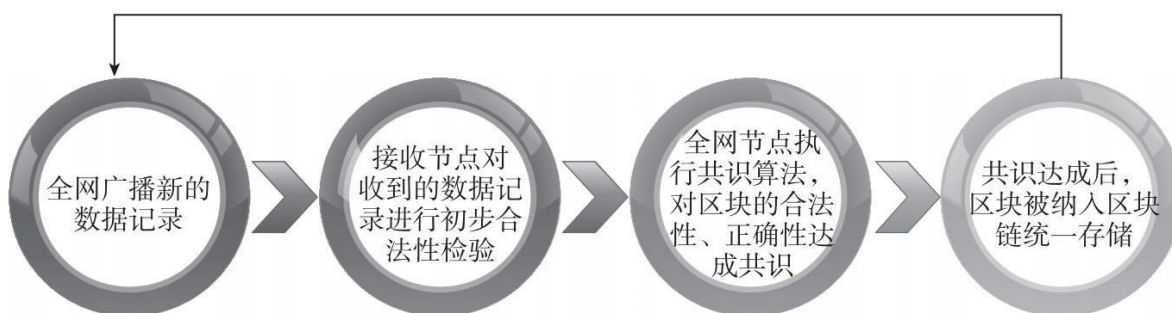


图2-6 区块链的工作流程

节点始终都将最长的区块链视为正确的链，并持续以此为基础验证和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别，它们将在先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成长的链条。该僵局的打破需要共识算法的进一步运行，当其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。以上就是防止区块链分叉的整个过程。

所谓“新的数据记录广播”，实际上不需要抵达全部的节点。只要数据记录信息能够抵达足够多的节点，那么将很快地被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

现在我们都知道了区块链网络里的记账者是节点，节点负责把数据记录记到数据区块里，为了鼓励节点记账，系统会按照规则随机地对记账的节点进行奖励。那么如何保证不会有人制造假数据记录或者说如何保证造假数据记录不被通过验证？这就涉及时戳。这也正是区块链与众不同的地方。区块链不仅关注数据区块里的内容，也关注数据区块本身，把数据区块的内容与数据区块本身通过时间戳联系起来。时间戳为什么会出现？这是由区块链的性质规定的。节点把数据记入了区块，因此一个区块就相当于一页账簿，每笔数据在账簿中的记录可以自动按时

间先后排列，那么账簿的页与页怎么衔接起来？也就是说，这一个区块与下一个区块的继承关系如何断定就成为问题。于是时间戳就出现了。

时间戳的重要意义在于其使数据区块形成了新的结构。这个新的结构使各个区块通过时间线有序连接起来，形成了一个区块的链条，因此才称为区块链。区块按时间的先后顺序排列使账簿的页与页的记录也具有了连续性。通过给数据记录印上时间标签，使每一条数据记录都具有唯一性，从而使数据记录本身在区块和区块上的哪个位置上发生可以被精确定位且可回溯，也给其他的校验机制协同发挥作用提供了极大的便利和确定性，使整个区块链网络能够确定性地验证某条数据记录是否真实。由于区块链网络是公开的，意味着系统知道过去发生的所有数据记录，而任何新的数据记录都继承于过去的的数据记录，因为过去的的数据记录是真实的，而且链条的各个区块记录由时间戳连接起来使之环环相扣，所以如果想要制造一个假的数据记录，就必须在区块链上修改过去的所有数据记录。尽管在挖矿的过程中，形成了多个链条，但因为最长的那个被诚实的节点所控制，所以想要修改过去的数据记录，首先就要从头构造出一个长度比之前最长的那个还要长的链条，在这个新的链条超过原来的那个链条后，才能制造双重支付的虚假数据。然而随着时间推移，制造新链条的难度和成本都是呈指数级上升的，而且随着链条越来越长，其难度也變得越来越大，成本也就越来越高。同时，因为去中心化的设置，区块链的各个核心客户端同时又是服务器，保存了区块链网络的完整数据，因此使对区块链网络的攻击很难像对传统的中央处理节点那样有效，一般情况下很难对区块链网络构成重大冲击。最终，区块链网络成为一个难以攻破的、公开的、不可篡改数据记录和制造虚假数据的诚实可信系统。

区块链保证数据安全、不可篡改以及透明性的关键技术包括两个方面：一是数据加密签名机制；二是共识算法。在数据加密签名机制中，首先，要有一个私钥，私钥是证明个人所有权的关键，比如证明某人有权从一个特定的钱包消费数字货币，是通过数字签名来实现的。其次，

要使用哈希（Hash）算法。哈希散列是密码学里的经典技术，把任意长度的输入通过哈希算法计算，变换成固定长度的由字母和数字组成的输出，具有不可逆性。共识算法是区块链中节点保持区块数据一致、准确的基础，现有的主流共识算法包括工作量证明（PoW）、权益证明（PoS）、瑞波共识协议（RCP）等。以PoW为例，是指通过消耗节点算力形成新的区块，是节点利用自身的计算机硬件为网络做数学计算进行交易确认和提高安全性的过程。交易支持者（矿工）在电脑上运行比特币软件不断计算软件提供的复杂的密码学问题来保证交易的进行。作为对他们服务的奖励，矿工可以得到他们所确认的交易中包含的手续费，以及新产生的比特币。

三、区块链共识机制

区块链要成为一个难以攻破的、公开的、不可篡改数据记录的去中心化诚实可信系统，需要在尽可能短的时间内做到分布式数据记录的安全、明确及不可逆，提供一个最坚实且去中心化的系统。在实践中，该流程分为两个方面：一是选择一个独特的节点来产生一个区块；二是使分布式数据记录不可逆。实现上述流程的技术核心就是：共识机制。共识机制是区块链节点就区块信息达成全网一致共识的机制，可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

当前主流的共识机制包括：工作量证明、权益证明、工作量证明与权益证明混合（PoS+PoW）、股份授权证明、瑞波共识协议等。

（一）工作量证明

工作量证明（Proof of Work），顾名思义，即指工作量的证明。PoW机制的基本步骤如下：①节点监听全网数据记录，通过基本合法性验证

的数据记录将进行暂存；②节点消耗自身算力尝试不同的随机数，进行指定哈希计算，并不断重复该过程直至找到合理的随机数；③找到合理的随机数后，生成区块信息，首先输入区块头信息，然后是数据记录信息；④接单对外部广播出新产生的区块，其他节点验证通过后，连接至区块链中，主链高度加一，然后所有节点切换至新区块后面继续进行工作量证明和区块生产。

PoW叫工作量证明体现在步骤②中，节点需要不断消耗算力工作，进行哈希计算，以找到期望的随机数。以比特币区块链为例，通过PoW机制维护区块链的整体运行及其安全性。验证节点通过随机的散列运算，争夺比特币区块链的记账权，防止欺诈交易，避免“双重支付”，这一过程需要消耗电力、算力来完成。因此，验证节点也成为“矿工”，随机数计算查找过程称为“挖矿”。每一个比特币区块链中的区块都包含着一个由无意义数据构成的短字符串（称为随机数），找到一个合适的随机数唯一已知的方法是不停地随机试探直到搜索到一个有效的数。比特币的PoW中，平均每10分钟有一个节点找到一个区块。如果两个节点在同一个时间找到区块，那么网络将根据后续节点和区块生成情况来确定哪个区块构建最终区块链。一般情况下，需要6个区块的生成时间进行确认，因为一般交易在6个区块（约1个小时）后被认为是安全确认且不可逆的。其工作量主要体现在：一个符合要求的区块随机数由N个前导零构成，零的个数取决于网络的难度值。要得到合理的随机数需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供一个合理的随机数值，说明该节点确实经过了大量的尝试计算。当然，这并不能得出计算次数的绝对值，因为寻找合理随机数值是一个概率事件。工作量证明机制看似很神秘，其实在社会中的应用非常广泛。例如，毕业证、学位证、律师证等证书就是工作证明，拥有证书即表明在过去付出了努力。挖矿为整个系统的运转提供原动力，挖矿有三个重要功能：一是发行新的货币；二是维系系统的支付功能；三是通过算力保障系统安全。首先，挖矿消耗资源将黄金注入流通经济，比特币通过“挖矿”完成相同的事情，只不过消耗的是CPU时间与电力。其次，挖

矿用于产量调节，区块的产量为大约每两周2016个，即每10分钟一块。第三，通过算力保障系统安全。算力攻击的概率难度呈指数上升（泊松分布），每个区块都必须指向前一个区块，否则无法验证通过。追根溯源便是高度为零的创世区块。PoW机制存在两方面明显的缺陷。一是算力的消耗与浪费。在PoW中，尽管区块链节点是用来帮区块链进行分布式数据记录的，但是它们实际所做的大部分工作是寻找正确的随机数而与数据记录无关。用来寻找随机数的能量和资源将永远地消失，这显然是一种浪费。二是算力集中化凸显。PoW机制自然地导致了算力集中问题。由于作为一个普通的个体或者几十、几百台规模的矿机目前都很难挖到区块了，因此大家必须联合起来挖矿，就诞生了算力集中的地方——矿池。其中最著名的是比特币Ghash矿池，它因为数次接近甚至达到了50%比特币的算力，从而引起了比特币社区的广泛担忧。

（二）权益证明+工作量证明

2012年8月，一个化名Sunny King的极客推出了Peercoin（PPC），采用工作量证明机制PoW发行新币，采用权益证明机制PoS维护网络安全，即PoW+PoS机制。该机制中，区块被分成两种形式——PoW区块及PoS区块。在这种新型区块链体系里，区块持有人可以消耗他的币天获得利息，同时获得为网络产生一个区块和用PoS造币的优先权。PoS的第一次输入被称为权益核心，需要符合某一哈希目标协议。因此，PoS区块的产生具有随机性，其过程与PoW相似。但有一个重要的区别在于，PoS随机散列运算是在一个有限制的空间里完成的，而不是PoW那样在无限制的空间里寻找，因此无须大量的能源消耗。权益核心所要符合的随机散列目标是以在核心中消耗的币天的目标值（币×天），这与PoW是不同的，PoW的每个节点都具有相同的目标值。因此，核心消耗的币天越多，就越容易符合目标协议。PoS中还有一种新型的造币过程。PoS区块将根据所消耗的币天产生利息币，设计时设定了每币一年将产生1分利息，以避免将来的通胀。在造币初期时保留了PoW，使最初的造币更加方便。

在区块链中谁是主链的问题是解决分叉的关键。PoS判断主链的标准已经转化为对消耗币天的判断。每个区块的交易都会将其消耗的币天提交给该区块，以提高该区块的得分。获得最高消耗币天的区块将被选中为主链。此设计减少了部分对于51%攻击的忧虑，因为在PoS区块中，要进行51%攻击，首先，要控制数量众多的币天，成本可能要高于获得51%的算力，这样就提高了攻击的成本；其次，攻击者在攻击网络时，其币天也会消耗，这将使攻击者阻止交易进入主链的行为变得更加困难。

为抵御分布式拒绝服务攻击，在PoW+PoS机制中，每个区块都必须由其拥有者签名，以避免受到复制并被攻击者使用。为了抵御攻击者复制产生多个区块进行分布式拒绝服务攻击，每个节点都会收集其接触到的（核心，时间戳）配对信息。假如一个已接收到的区块包含与其他之前收到的区块中的配对信息（核心，时间戳）是重复的，会忽略此区块直到后者被孤立出去。

在PoW+POS机制下，只要持有币的人，不论持有的数量多少，都可以挖到数据块，而不用采用任何的矿池导致算力集中。同时，由于多采用币天生成区块，而不是算力，降低了资源消耗，解决了单纯PoW机制在维护网络安全方面先天不足的问题。

（三）权益证明

除了结合PoW使用外，能否单独利用PoS机制进行区块链系统设计运行呢？答案是肯定的。简单来说，PoS就是一个根据持有货币的量和时间，进行利息发放和区块产生的机制。在权益证明PoS模式下，有一个名词叫币天。例如，每个币每天产生1币天，比如持有100个币，总共持有了30天，那么此时币天就为3000。这个时候，如果发现了一个新PoS区块，币天就会被清空为0。每被清空365币天，将会从区块中获得0.05个币的利息（可理解为年利率5%）。

PoS的典型应用就是未来币。同其他加密货币一样，未来币体系的总账是建立和储存在一系列区块里的，也就是区块链中。每个区块链的备份都存放在未来币网络的每个节点里，而且在每个节点上没有加密的每个账户都能够生成区块，只要至少一个新入账户的交易已经确认了1440次。任何账户只要达到了这个标准就会被视为“激活账户”。在未来币里，每个区块都包含着255个交易，每个交易都是由包含识别参数的192字节的数据头开始的。一个区块里的每个交易量都是由128个字节所代表着。总共加在一起就意味着最大的区块大小有32K字节。每个区块都有一个“生成签名”的参数。激活账户用自己的私钥在原先的区块上签署“生成签名”。这就产生了一个64字节的签名，之后通过SHA256散列该签名。哈希产生的前八个字节给出了一个数字，作为一个“hit”。“hit”与目前的目标值相比较，如果计算出的“hit”值要比“目标值”低，那么就可以生成下一个区块了。对于每个活动账户来讲，“目标值”都是与它自身所确认的余额成比例的。一个持有1000个币的账户得到的目标值是持有20个币账户所得到目标值的50倍。因此，拥有1000个币的持有者产生的区块数是持有20个币的人产生的50倍。同时，“目标值”并不是固定的，随着先前区块的时间戳的流逝时刻都在增长。如果在最初的一秒钟内没有哪个账户的“hit”值是低于“目标值”的，则下一秒钟“目标值”就会翻倍。“目标值”会连续地翻倍，直到一个活动账户的“hit”值有一个较低的数值。还有一个“基本目标”值，它以60秒的间隔设定为目标值。正是这个原因，一个区块平均产生的时间会在60秒。即使在网络上只有很少的激活账户，它们其中的一个最终会产生一个区块因为“目标”值会变得相当大。通过将你账户的“hit”值与目前的“目标”值相比，你就可以估算出你的“hit”值还有多久能成功。

当一个激活账户赢得产生区块的权利时，就能将任何可获得的且未确认的交易放入区块中，并用所有需要的参数来填充该区块。然后，这个区块就会被传播到网络中作为一个区块链的备选。每一个区块中的负载值、“hit”、产生的账户以及签名都能被网络上接收到它的节点所确认。每个区块参考之前的区块，区块形成的区块链可以用来追溯和查询

网络中素有的交易历史，所有这些都会追溯到创世源区。上述完整地展示了利用币天进行区块产生和验证共识的过程，体现了PoS的核心思想。

（四）股份授权证明

PoS机制使用一个确定性算法以随机选择一个股东来产生下一个区块，该算法中，账户余额决定了节点被选中的可能性。然而，该系统并未使区块链变得越来越安全而不可逆，因为最终区块链的区块产生权掌握在账户余额最多的少数节点手中。同时，PoS面临的挑战是如何通过及时而高效的方法达成共识。为达到这个目标，每个持币节点可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每名代表被分配到一个时间段生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的1%作为报酬。如果一个平均水平的区块含有100股作为交易费，一名代表将获得1股作为报酬，即可大大提高共识效率。这就是DPoS的核心思想。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这发生的概率较小，因为制造区块的代表可以与制造前后区块的代表建立直接连接。在DPoS中，第一个步骤是成为一名代表，必须在网络上注册公钥，然后分配到一个32位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。第二个步骤是授权选票。每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。每个钱包将显示一个状态指示器，让用户知道代表的表现如何。如果某代表错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个

钱包进行更多交易前要求选出一个新代表。与PoW系统及其他PoS系统一样，最佳区块链是最长的有效区块链。在任何时候，一名代表错过签发一个区块的机会，该区块链将比潜在竞争对手短。只要交易被写入区块后的100个区块中的51%被生产出来了，那么你就可以安全地认为在主区块链上。也许，在防止区块链分叉所导致的损失方面，最重要的事是在事发后第一时间得知消息。如果10区块中有超过5个错过生产，那么这意味着你很可能在一条支链上，因此应该停止所有交易，直到分叉得到解决。以一种及时的方式（少于5分钟）简单地发现并警示用户网络分叉，是可以最小化潜在损失的非常重要的能力。

（五）瑞波共识协议

瑞波共识协议（Ripple Consensus Protocol, RCP），使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由一定比例的该俱乐部会员投票通过。RCP机制的工作原理如下。

①验证节点接收存储待验证交易。首先，验证节点接收待验证交易，将其存储在本地；其次，本轮共识过程中新到的交易需要等待，在下次共识时再确认。

②活跃信任节点发送提议：首先，信任节点列表是验证池的一个子集，其信任节点来源于验证池；其次，参与共识过程的信任节点须处于活跃状态，验证节点与信任节点间存在保活机制，长期不活跃节点将从信任节点列表删除；最后，信任节点根据自身掌握的交易双方额度、交易历史等信息对交易做出判断，并加入到提议中进行发送。

③本验证节点检查收到的提议是否来自信任节点列表中的合法信任节点，如果是，则存储；如果不是，则丢弃。

④验证节点根据提议确定认可交易列表的步骤如下：首先，令信任

节点列表中活跃的信任节点个数为M（比如5个），本轮中交易认可阈值为N（百分比，比如50%），则每一个超过 $M \times N$ 个信任节点认可的交易将被本验证节点认可；其次，本验证节点生成认可交易列表。系统为验证节点设置一个计数器，如果计数器时间已到，本信任节点需要发送自己的认可交易列表。

⑤账本共识达成的步骤如下：首先，本验证节点仍然在接收来自信任节点列表中信任节点的提议，并持续更新认可交易列表；其次，验证节点认可列表的生成并不代表最终账本的形成以及共识的达成，账本共识只有在每笔交易都获得至少超过一定阈值（比如80%）的信任节点列表认可才能达成。如果账本中每笔交易都获得至少超过一定阈值（比如80%）的信任节点列表认可，则共识达成，交易验证结束，否则继续上述过程。

⑥共识过程结束后，已经形成最新的账本，现将上轮剩余的待确认交易以及新交易纳入待确认交易列表，开始新一轮共识过程。

除上述机制外，还有恒星共识协议（Stellar Consensus Protocol, SCP）、改进型实用拜占庭容错机制（Practical Byzantine Fault Tolerance, PBFT）和Pool验证池机制等共识机制被提出，甚至已经应用在区块链系统中，不同共识机制各有其应用场景和优势。

四、区块链面临的问题

目前，区块链技术已经受到众多领域的广泛关注并得到应用，包括托管交易、金融交易、公共交易、证件、私人记录、留存证明、实物资产、无形资产等。然而，区块链技术在面临机遇的同时，也面临着不少问题与挑战。

（一）区块链体积过大问题

随着区块链的发展，节点存储的区块链数据体积会越来越大，存储和计算负担将越来越重。以比特币区块链为例，其完整数据的大小当前已达63.61GB（千兆）（图2-7），用户如果使用比特币核心客户端进行数据同步的话，可能三天三夜都无法同步完成，并且，区块链的数据量还在不断地增加。这给比特币核心客户端的运行带来了很大的困难。

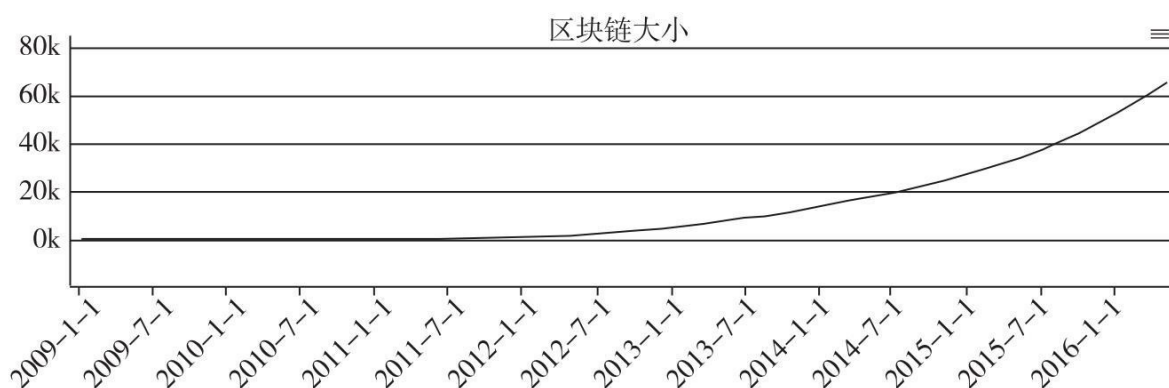


图2-7 比特币区块链体积增长趋势

数据来源：区块元blockmeta.com

（二）区块链数据确认时间的问题

目前的区块链系统，尤其是金融区块链系统中，存在数据确认时间较长的问题。以比特币区块链为例，当前比特币交易的一次确认时间大约需要10分钟（图2-8），6次确认的情况下，需要等待约1小时。当然，对于信用卡动则2~3天的确认时间来说，比特币已经有了很大的进步，但距离理想状态仍有较大距离。

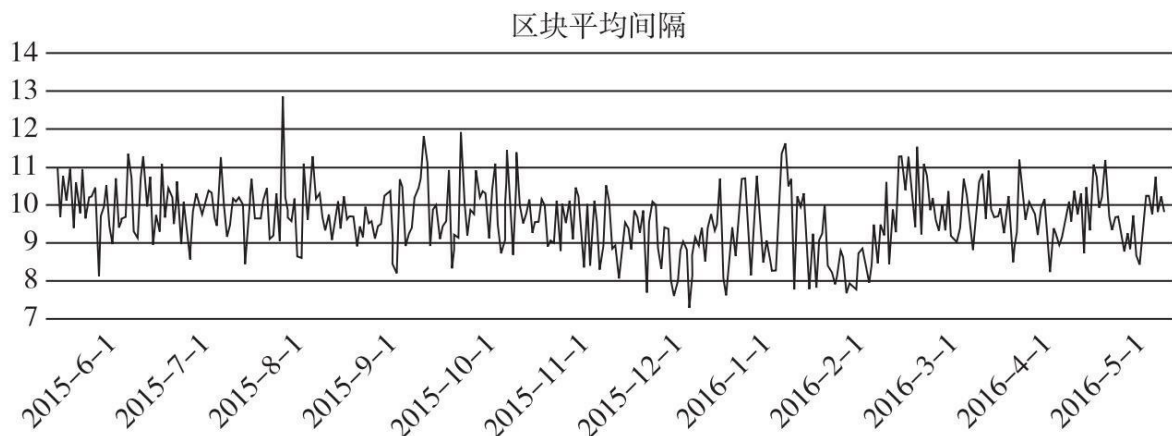


图2-8 比特币区块生产间隔

数据来源：区块元blockmeta.com。

（三）处理交易频率问题

区块链系统面临交易频率过低的问题。还是以比特币区块链为例，每条交易的平均大小约为250个字节（Byte），如果区块大小限制在1MB（兆），那么可以容纳的交易数量为4000条。按照每10分钟产生一个区块的速度计算，每天可以产生144个区块，也就是能容纳576000条交易，再除以每天的秒数86400，比特币区块链最高每秒处理6.67笔交易。目前，比特币区块链上每天的实际交易量已经接近系统“瓶颈”（图2-9），如果扩容问题得不到解决，可能造成大量交易的堵塞延迟。

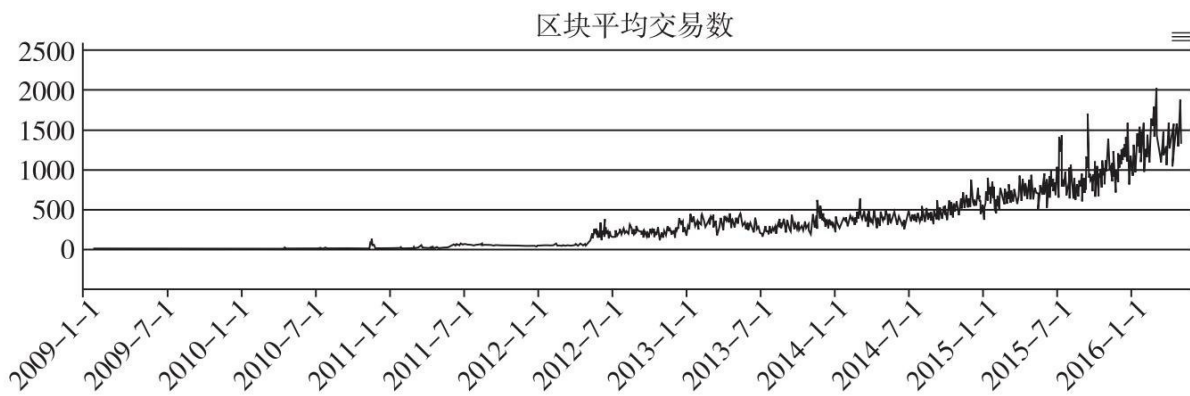


图2-9 比特币区块平均交易数

数据来源：区块元blockmeta.com。

相比之下，Paypal在2013年第三季度的总体交易笔数为7.29亿笔，平均每秒为93.75笔交易。全球最大的支付卡VISA的官网信息显示，VisaNet（维萨网）在2013年的测试中，实现了每秒处理47000笔交易。比特币区块链比起支付宝等几大支付网络，从交易处理频率来看，更像是一个刚出生的婴儿。当然，这也是中本聪早期故意为之的设计。比特币区块大小被限制在1MB，以此避免“流氓”矿工的恶意行为，对人们造成不良的影响。比特币区块链支付网络之所以能够成长到如今价值数十亿美元，就在于它的去中心化。

（四）区块链发展受到现行制度的制约

一方面，区块链去中心、自治化的特性淡化了国家监管的概念，对现行体制带来了冲击。比如，以比特币为代表的数字货币不但对国家货币发行权构成挑战，还影响到货币政策的传导效果，削弱央行调控经济的能力，导致货币当局对数字货币的发展保持谨慎态度。另一方面，监管部门对这项新技术也缺乏充分的认识和预期，法律和制度建立可能会滞后，导致与运用区块链相关的经济活动缺乏必要的制度规范和法律保护，无形中加大了市场主体的风险。

（五）区块链技术与现有制度的整合成本较大

对于任何创新，现有机构都要保证既能创造经济效益，又要符合监管要求，还要与传统基础设施相衔接。特别是当部署一个新型基础系统时，耗费的时间、人力、物力成本都非常大，现有传统机构内部遇到的阻力也不小。

当然，问题的存在并不能阻碍区块链的发展步伐，诸如简单支付验证、侧链、闪电网络协议等技术的提出和深入研究，已经为上述问题的解决提出了思路。

参考资料

- [1]<http://www.jianshu.com/p/5e06fee80460>
- [2]<http://www.zhihu.com/question/27687960/answer/70057319>
- [3]<http://www.8btc.com/on-public-and-private-blockchains>
- [4]<http://www.zhuihun.com/domainnews-20983-1-1.html>
- [5]<http://www.wanhuajing.com/d342166>
- [6]<http://www.zhihu.com/question/22369364/answer/21169413>
- [7]<http://8btc.com/thread-540-1-1.html>
- [8]<http://8btc.com/article-1882-1.html>
- [9]<http://www.8btc.com/what-proof-of-stake-is-and-why-it-matters/>
- [10]<http://www.8btc.com/fu0powpos> <http://www.8btc.com/nxt-whitepaper>
- [11]<http://coinfeed.net/cn/information/bitshares/dpos授权股权证明机制白皮书.html>
- [12]<http://www.8btc.com/blockchain-scalability>
- [13]<http://toutiao.com/i6243674242018181634/>

[15] 本章由海滨完成。海滨,布比公司技术专家、博士,在区块链技术、网络安全、数字货币等领域有非常深厚的技术积累。布比公司专注于区块链技术和产品的创新,已经拥有多项核心技术,开发了高可扩展高性能的区块链基础服务平台,具备快速构建上层应用业务的能力,满足数千万级用户规模的场景。

[16] 范捷,易乐天,舒继武.拜占庭系统技术研究综述 [J] .软件学报, 2013 (6) :12.

[17] 巴比特.比特币与拜占庭将军问题, <http://www.8btc.com/baizhantingjiangjun>.

第三章

区块链进阶^[18]

一、简单支付验证（SPV）

简单支付验证（Simplified Payment Verification，简称SPV）是一种无须维护完整的区块链信息，只需要保存所有的区块头部信息即可进行支付验证的技术。该技术可以大大节省区块链支付验证用户的存储空间，减轻用户存储负担，降低区块链未来交易量剧增而给用户带来的压力。以比特币系统为例，节点只需保存所有区块头信息，即可进行交易支付验证。节点虽然不能独立验证交易，但能够从区块链其他节点获取交易验证的必要信息，从而完成交易支付验证，同时还可以得到整个区块链网络对交易的确认数。

要理解SPV的概念，首先需要理解如下两类概念的区别。

一是SPV与轻钱包（或瘦客户端）的区别。轻钱包指的是节点本地只保存与其自身相关的交易数据（尤其是可支配交易数据），但并不保存完整区块链信息的技术。SPV的目标是验证某个支付是否真实存在，并得到了多少个确认。比如爱丽丝（Alice）收到来自鲍伯（Bob）的一个通知，鲍伯声称已经从其账户中汇款一定数额的钱给了爱丽丝。如何快速验证该支付的真实性，是SPV的工作目标。轻钱包或瘦客户端的目标不仅是支付验证，而且是用于管理节点自身的资产收入、支付等信息。比如爱丽丝使用轻钱包或瘦客户端管理自身在区块链的收入信息、支出信息，在本地只保存与爱丽丝自身相关的交易数据，尤其是可支配交易数据。轻钱包与SPV的最大区别是，轻钱包节点仍需下载每个新区

块的全部数据并进行解析，获取并本地存储与自身相关的交易数据，只是无须在本地保存全部数据而已。而SPV节点不需要下载新区块的全部数据，只需要保存区块头部信息即可。虽然轻钱包或瘦客户端中部分借鉴了SPV的理念，但和SPV是完全不同的。

二是区块链支付验证与区块链交易验证的区别。SPV指的是区块链支付验证，而不是区块链交易验证。这两种验证方式存在很大的区别。区块链交易验证的过程比较复杂，包括账户余额验证、双重支付判断等，通常由保存区块链完整信息的区块链验证节点来完成。而支付验证的过程比较简单，只是判断该笔支付交易是否已经得到了区块链节点共识验证，并得到了多少的确认数即可。还是以比特币系统为例，用户爱丽丝收到来自鲍伯的通知，鲍伯声称已经从其账户中汇款一定数额的钱给爱丽丝。爱丽丝进行交易验证的过程如下：首先，爱丽丝遍历完整的区块链账本，在区块链账本的交易中保存了鲍伯的历史交易信息（包括鲍伯的汇款账户、鲍伯的签名、历史收款人的地址以及汇款金额信息等），查询鲍伯的账户，就可以判断鲍伯提供的账户是否有足够的余额，如果余额不足则交易验证失败；其次，爱丽丝要根据区块链账本判断鲍伯是否已经支出了这个账户上的钱给别人，即是否存在双重支付问题，如果存在则交易验证失败；最后，判断鲍伯是否拥有其提供账户的支配权，如果判断失败则交易验证失败。而如果爱丽丝只是进行支付验证，则过程简单得多：通过SPV，爱丽丝可以进行支付快速验证，即检查此项支付交易是否已经被收录存储于区块链中，并得到了多少个确认数，就可以判断支付验证的合法性。详细的技术原理如下。

（一）SPV的技术原理

在区块链中，区块信息主要包括区块大小、区块头、交易数量和交易信息四部分内容。其中，区块头大小为固定字节，比如比特币中区块头的大小始终为80字节。区块头中一般包括如下信息：前一区块（也称父区块）的哈希值、区块中交易默克尔树的根哈希值、时间戳等。以比

特币为例，其区块头的数据结构如表3-1所示。

表3-1 区块头的数据结构

字段	描述	字节数
版本	软件协议版本号	4 字节
前一区块的哈希值	也称父区块的哈希值，为区块链中前一区块的哈希值	32 字节
默克尔树根	区块中所有交易信息生成的默克尔树的根哈希值	32 字节
时间戳	区块生成时间	4 字节
难度	工作量证明的难度目标	4 字节
Nonce（随机数）	用于工作量证明算法的计数器	4 字节

通过区块的哈希值，可以识别出区块链中的对应区块。区块前后有序链接，每一个区块都可以通过其区块头的“前一区块的哈希值”字段引用前一区块。这样把每个区块均链接到各自前一区块的哈希值序列就创建了一条一直可以追溯到第一个区块（创世区块）的链条。前一区块的哈希值，可以确保区块链所记录的交易次序。默克尔树的根哈希值则可以确保收录到区块中的所有交易的真实性。

区块链节点利用SPV对支付进行验证的工作原理如下：

- ①计算待验证支付的交易哈希值；
- ②节点从区块链网络上获取并存储最长链的所有区块头至本地；
- ③节点从区块链获取待验证支付对应的默克尔树哈希认证路径；
- ④根据哈希认证路径，计算默克尔树的根哈希值，将计算结果与本地区块头中的默克尔树的根哈希值进行比较，定位到包含待验证支付的区块；

⑤验证该区块的区块头是否已经包含在已知最长链中，如果包含则证明支付真实有效；

⑥根据该区块头所处的位置，确定该支付已经得到的确认数量。

上述方法可以减轻用户的负担。以比特币为例，无论未来的交易量多大，区块头的大小始终只有80字节，按照每小时6个的区块生成速度，每年产出52560个区块。当只保存区块头时，每年新增存储需求约为4兆字节，100年后累计的存储需求仅为400兆字节，即使用户使用的是最低端的设备，正常情况下也完全能够负载。

SPV的工作原理中，最为关键和复杂的是步骤③，节点从区块链获取待验证支付对应的默克尔树哈希认证路径的过程。例如，一个区块链节点想要知道其钱包中某个比特币地址即将到达的某笔支付，该节点会在节点间的通信链接上建立起布鲁姆过滤器，限制只接受含有目标比特币地址的交易。当节点探测到某交易符合布鲁姆过滤器的要求时，将以默克尔区块消息的形式发送该区块。默克尔区块消息包含区块头和一条连接目标交易与默克尔树根的默克尔哈希认证路径。默克尔树哈希认证路径是验证待验证支付是否存在于默克尔树的关键条件，该认证路径由默克尔树所有路径中节点的哈希值共同构成，自下而上进行哈希计算。节点能够使用该路径找到与该交易相关的区块，进而验证对应区块中该交易的有无。如图3-1所示为根据交易A、B、C、D、E、F、G、H生成的默克尔树。这是一棵自下而上通过哈希运算生成的二叉树。叶子节点为交易信息的哈希值，叶子节点两两进行哈希运算得到其父节点，继续此过程，直至生成默克尔树根节点。需要注意的是，如果存在单个叶子节点无法匹配成对，则用复制的方法构成完整的二叉树，比如图3-2中交易H不存在，则可以将交易G的哈希值 $M(G)$ 复制一份替代 $M(H)$ ，从而完成二叉树的生成过程。

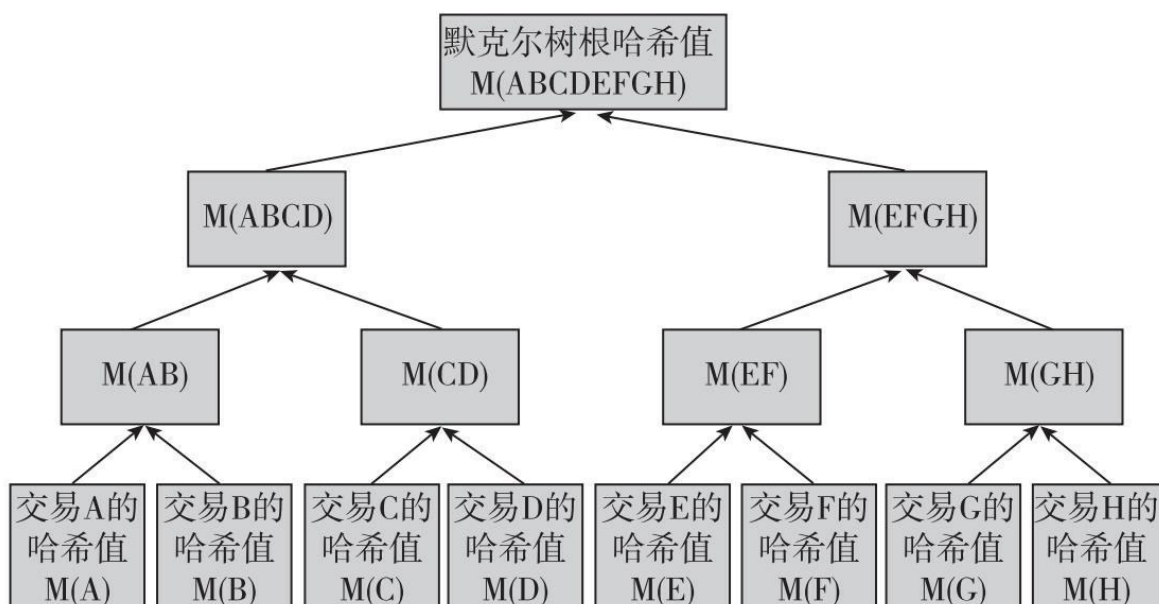


图3-1 交易默克尔树结构示意图

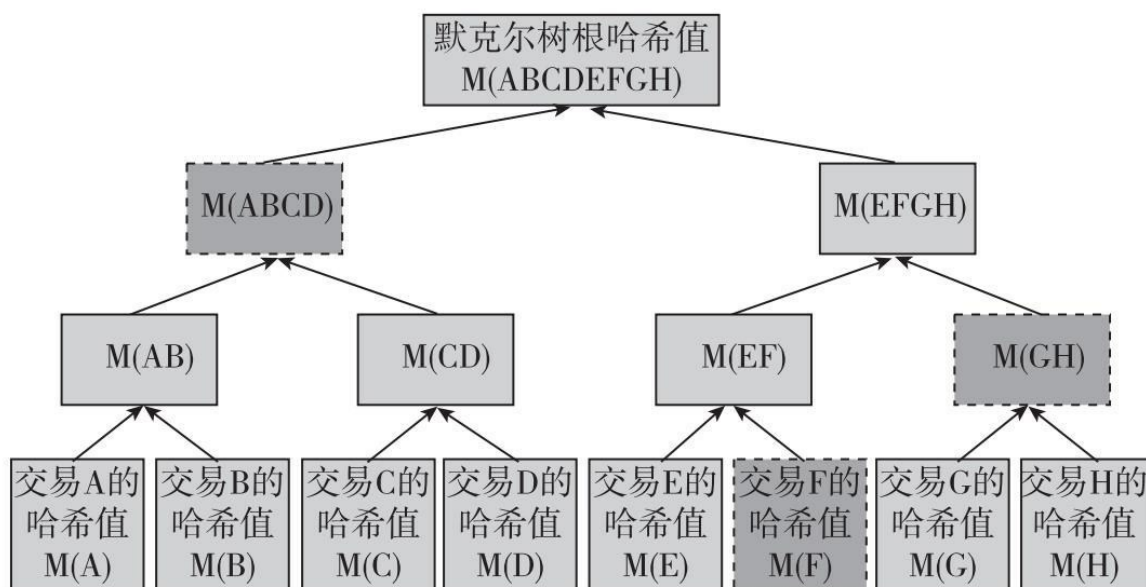


图3-2 默克尔树哈希认证路径示意图

假设待验证交易为E，则交易E的默克尔树哈希认证路径为图3-2虚线框所示的M(F)、M(GH)和M(ABCD)。通过该哈希认证路径，即可以通过哈希计算找到一条链接交易E与默克尔树根的完整路径。

（二）SPV的功能扩展

虽然SPV可以高效地进行支付验证，但对于节点当前状态（账户余额、账户信息甚至合约状态等）均无法给出证明。SPV能否扩展并更进一步呢？以太坊对SPV的功能进行了扩展：每一个区块头，并非只包含一棵默克尔树，而是包含了三棵默克尔树，分别对应了三种对象——默克尔交易树、默克尔收据树和默克尔状态树。其中默克尔收据树和默克尔状态树是比特币等现有区块链系统没有的。默克尔收据树是由展示每一笔交易影响的数据条构成的默克尔树。而在默克尔状态树中，则保存账户信息、账户余额等信息。三棵默克尔树的功能分工如下。

①默克尔交易树：保存交易信息，用于验证交易是否真实包含于区块链中。

②默克尔收据树：保存某个地址的历史事件实例，比如一个交易是否成功执行、一个众筹合约是否完成了目标等。

③默克尔状态树：保存了账户名称、账户余额等信息。

基于上述三棵树，以太坊不仅可以实现SPV的支付验证，而且可以快速验证账户是否存在、了解账户余额甚至快速判断交易是否执行成功等信息，实现了良好的SPV扩展。

（三）SPV面临的问题

SPV面临的第一个问题是SPV节点与区块链系统去中心化程度似乎存在一定的矛盾。随着SPV节点数量的增多，那么区块链参与完整验证的节点数量就会减少。然而，SPV却不能完全独立构成区块链。由于SPV节点没有存储完整的区块链信息，SPV的实现离不开存储区块链完整信息的节点或系统的辅助。

SPV面临的第二个问题是交易可锻性攻击[\[19\]](#)。由于SPV实现中一个关键步骤是根据支付哈希值定位其在区块中的位置，而该过程可能遭遇交易可锻性攻击。比如比特币系统中，交易可锻性攻击体现在交易ID（账号）可被伪造，而交易ID可被伪造的原因是比特币签名算法不够完善。以比特币为例，交易可锻性攻击的过程如下：在比特币的交易中，第三方交易系统会将交易发送方、接受方、交易金额等数据作为一个交易发送到比特币网络中，发送之前会对这条交易信息进行加密和签名，接着根据生成的签名最终获得一个哈希值，这个哈希值作为交易ID返回给提现的用户。一次交易请求过后，用户接收到的仅有一个交易ID，根据这个交易ID可以查看交易是否成功。当交易发送到比特币网络中后，网络中的各个节点会根据之前生成的签名来验证交易的真实性。问题就出在签名算法上：椭圆曲线数字签名ECDSA这个算法的一个问题是，修改签名的某个字节能够使签名依然校验成功，这样伪造签名之后交易依然能够成功进行。由于交易ID是根据签名生成的，而伪造之后的签名会生成一个完全不同的交易ID，第三方判断到两个ID不同便会确定当前交易失败，而事实上交易已经成功了。这时如果用户发现交易提示失败，可以再次发起交易，第三方交易系统一看之前交易确实失败了，那就会再进行一次交易。这时用户的比特币钱包里就会多收到一份比特币，也就造成了第三方交易平台资金损失。交易的可锻性体现在虽然交易签名被“锻造过”（即修改伪造过），但最终的交易依然有效。上述攻击对于SPV是有效的，因为在交易可锻性攻击场景中，伪造的交易和正常的交易都在区块链网络中，如果伪造的交易先被处理，那么攻击就成功。从而，SPV支付在区块链中的位置定位过程可能无法完成或出现错误，最终影响支付验证的进程和准确性。

有人提出可以通过改进SPV的工作流程来提升攻击防范的有效性，比如不再仅根据哈希值来判断支付的状态，而是使用双因素或者多因素验证，包括账户余额、支付信息追踪等来综合判断支付是否真正成功，但这会增加SPV的复杂度。如何更加有效地解决SPV面临的问题还值得

进一步研究。

二、侧链

（一）侧链的起源

侧链（sidechains）实质上不是特指某个区块链，而是指遵守侧链协议的所有区块链，该词是相对于比特币主链来说的。侧链协议是指可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。

显然，只需符合侧链协议，所有现存的区块链，如以太坊、莱特币、暗网币等竞争区块链都可以成为侧链。元素链（Elements）就是这样一种侧链。所不同的是，它是由BlockStream公司，即提出侧链协议的公司开发的一个侧链的参考实现。

侧链协议具有重大意义。它意味着比特币不仅可以在比特币区块链上流通，还可以在其他区块链上流通，其应用范围和应用前景会更加广泛；有创意的人们会研发出各种各样的应用以侧链协议与比特币主链对接，使得比特币这种基准自由货币的地位更加牢固。

侧链协议的产生有以下几个原因。

1.应对其他区块链的创新威胁

以太坊（Ethereum）区块链、比特股（Bitshares）区块链后来居上，对比特币区块链产生相当大的威胁。智能合约和各种去中心化应用在以上两个区块链上兴起，受到人们的欢迎。而基于比特币的应用则因为开发难度大，项目不多。

2.比特币核心开发组不欢迎附生链

比特币区块链也有合约币（Counterparty）、万事达币（Mastercoin）和彩色币（ColoredCoin）等附生链，但是比特币核心开发组并不欢迎它们，觉得它们降低了比特币区块链的安全性。他们曾经一度把OP_RETURN的数据区减少到40字节，逼迫合约币开发团队改用其他方式在比特币交易中附带数据。

3.BlockStream商业化考虑

2014年7月以太坊众筹时，获得了价值1.4亿元人民币的比特币，还有20%的以太币，开发团队获得了巨大的回报。但是比特币核心开发组并没有因为他们的辛勤工作获得可观回报，因而他们成立了BlockStream，拟实现商业化价值。

基于以上三个原因，提出侧链协议、把比特币转出比特币区块链、另行开发二代区块链，这样的选择既能保证比特币区块链的安全，又能应对二代币的冲击，还能针对不同应用场景实现商业化，因而成了BlockStream的必然选择。

（二）侧链协议

侧链协议的目的是实现双向锚定（Two-way Peg），使比特币可以在主链和侧链中互转（图3-3）。

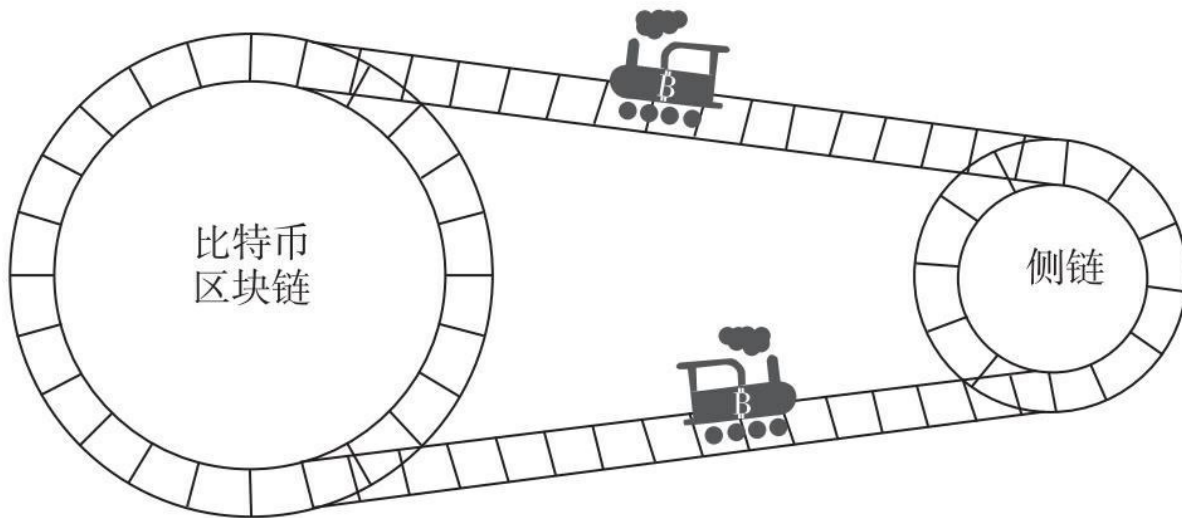


图3-3 比特币主链与侧链关系图

双向锚定分为以下几个阶段（图3-4）。

1.发送锁定交易，把比特币锁定在主链上

由比特币持有者操作，发送一个特殊交易，把比特币锁定在区块链上。

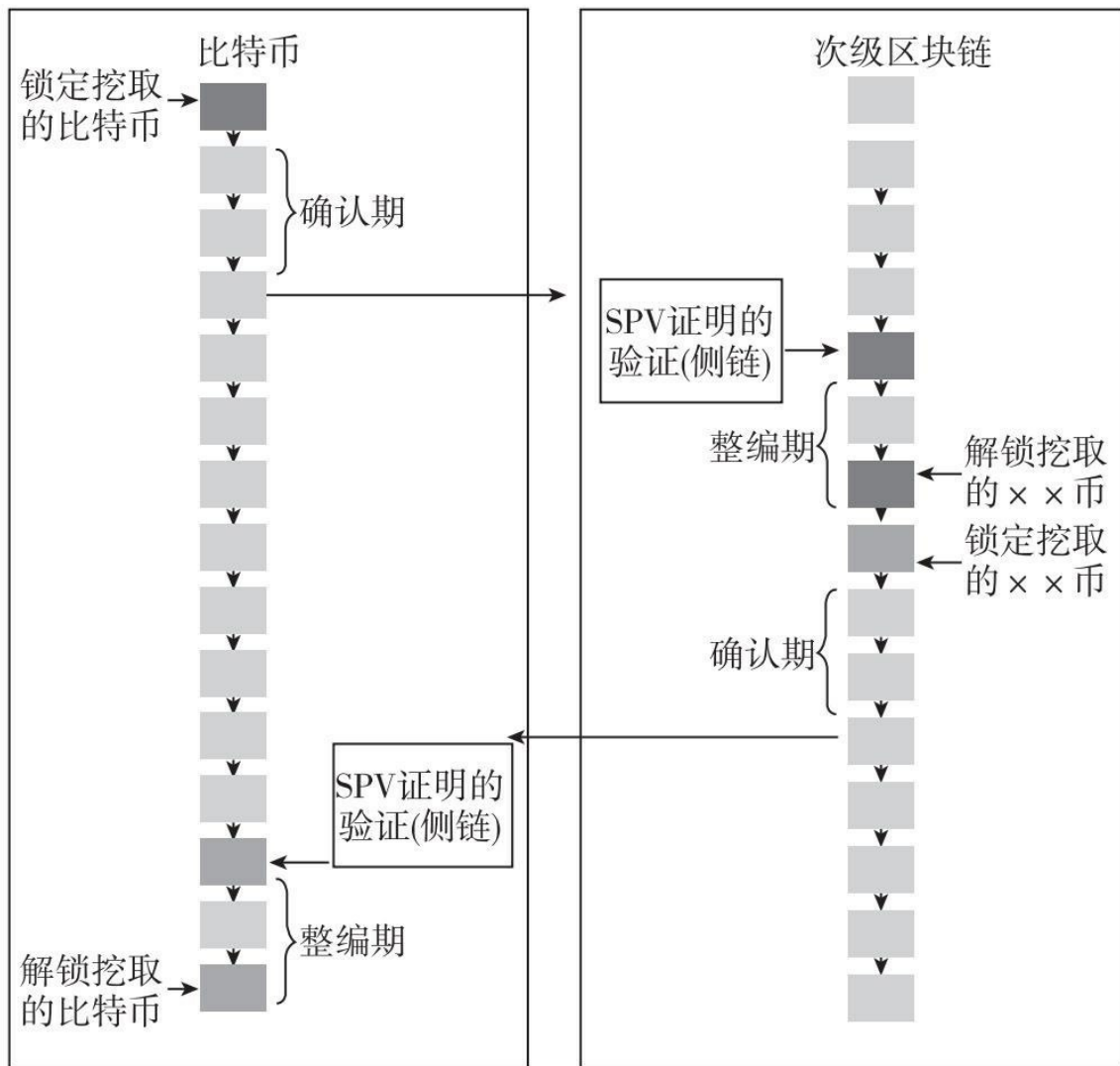


图3-4 双向锁定示意图

2.等待确认期

确认期的作用是等待锁定交易被更多区块确认，可防止假冒锁定交易和拒绝服务攻击，等待时间是1~2天。

3.在侧链上赎回比特币

确认期结束后，用户在侧链上创建一个交易花掉锁定交易的输出，并且提供一个SPV工作量证明，输出到自己在侧链上的地址中。该交易

称为赎回交易，SPV工作量证明是指赎回交易所在区块的工作量证明。

4.等待一个竞争期

竞争期的作用是防止双重支付。在此期间，①赎回交易不会被打包到区块；②新传输到侧链的比特币不能使用；③如果有工作量更大的工作证明出现，即该赎回交易包括了比特币主链更大难度的SPV证明，则上一个赎回交易将被替换。

竞争期结束后，该赎回交易将被打包到区块中，用户可以使用自己的比特币。

从侧链转比特币到主链的过程也是如此。这就是侧链双向锚定协议。

（三）元素链

元素链是BlockStream实现的一个参考侧链，Alpha（阿尔发）版于2015年7月推出。元素链Alpha旨在演示技术并且提供测试环境，目前还未开发完成。作为一个与比特币测试网络相对接的侧链，元素链Alpha有可能被其他技术取代。

元素链Alpha是比特币测试链的一个侧链。它依赖可审计的联合签名者来管理传输到侧链的测试币（参见确定性锚定特性），并且以此来产生签名区块（参见签名区块特性）。这样做能快速探索侧链实施的可能性，考虑如何使用不同的安全措施。在未来版本中，升级协议接口以完全支持去中心化的侧链联合挖矿，最终达到完全双向锚定的目标。

元素链所包括的技术如下。

1.私密交易

元素链中最具创新意义的特性莫过于私密交易。私密交易中的金额仅有该交易的参与者知道（或者参与者指定的人），元素链以密码学算法保证不会多花币。比特币用地址来保证隐私，同时公开交易让别人验证；元素链在保护个人隐私上更进一步，隐藏了交易金额。金额隐藏的具体技术见下文。

私密交易最明显的一点是引入了一种新地址类型，称为私密地址。私密地址含了一个盲化因子，比普通比特币地址更长，这种地址在元素链Alpha版本中是默认地址。

2.隔离见证

Alpha版的交易中，签名从交易中分离出来。此举完全消除了任何已知形式的交易可塑性的威胁，并且允许有效的区块链剪枝。

在比特币中，交易包含转账信息（未花费交易集、地址和金额）和用于证明交易合法性的签名；对于隔离见证来说，交易ID仅由转账信息生成，区块中包含签名。这样做有如下好处：

①比特币有一些“正常化交易ID”的建议，隔离见证包含了这些建议。因为正常化交易ID机制在可塑性的输入后还要重写所依赖的交易，对高层协议如闪电网络来说是必要基础。

②交易ID不覆盖签名，以比BIP62更好的方式，避免了交易可塑性的所有形式，而后可以安全地使用更大尺寸的多语句智能合同。

③具有更有效提供SPV证明（用于轻钱包）的潜力，因为签名可以从交易中被省略而不破坏默克尔树结构。节点无须存贮或验证签名，可以把签名从磁盘中删除或无须在网络上传输它，以大幅度减少区块链存储容量和宽带要求。但在Alpha版本中，证明数据比比特币签名更占空间，因为还包含了大段的输出金额证明（因为使用了私密交易，隐藏了

金额，因而要使用密码学证明以防止多花）。

3.相对锁定时间

为序列号赋予了新的意义，使已签名交易被确认后，其输入在一段特定时间内保持无效，目的是支持交易替换功能。

比特币每个交易都有个序列号，初始想法是相比低序列号，最高序列号应该最占优势，矿工应该更喜欢它，但这个想法从未真正实现。在假设矿工利益最大化的前提下，为了使得交易替换机制得以加强，新增一个操作码CHECKSEQUENCEVERIFY，用于比特币脚本检查序列号限制。

相对锁定时间与常规锁定时间用途一致，如时间锁定的担保服务等。但所指的“相对”会使以区块链为媒介的应用更有意思。例如双向锚定阶段可描述为以交易开始的一个相对锁定时间条件，该交易声明了赎回证据。

4.Schnorr签名验证

元素链未使用ECDSA签名方案，而使用了同一曲线上的Schnorr签名方案。其好处如下。

①更有效的n/n阈值签名。多个Schnorr签名可以被合成一个签名，该签名对公钥的总和来说是有效的，所以任意大的n/n多签名只需用一个合签名就可以完成，同时可以被一个CHECKSIG操作所验证。

②更小的签名容量（64字节，而非71~72字节），没有DER编码问题。潜在支持批量验证（同时验证32个签名达到最高2倍加速），这要知道R.y坐标（ECDSA忽略这个参数）和脚本级别，确保所有签名验证错误导致脚本运行错误（比如所有CHECKSIG操作与CHECKSIGVERIFY类似），以便提供更强的安全证明。

③能证明没有固有的签名可塑性问题。ECDSA有可塑性问题，并且不知道是否存在其他形式的可塑性问题。注意，分离证据使得签名可塑性不会导致交易可塑性。

④比ECDSA的签名和验证速度更快一点。

5.新操作码

元素链Alpha版本新增几个新脚本操作码。

①被禁用的操作码。比特币以前支持许多操作码，一些操作码在2010年因为安全考虑被禁用，需要硬分叉才能重新启用。Alpha版本重新启用了一些被禁用但是安全的操作码，如字符串连接和字符串操作码，整数位移码和几个位操作码。

②DETERMINISTICRANDOM操作码：根据种子在一个范围内产生一个随机数。

③CHECKSIGFROMSTACK操作码：验证堆栈中对消息的签名，而不是验证对交易本身的签名。

这些新操作码有一些使用场景，包括双花保护债券、彩票、允许1/N多签名的默克尔树结构（N可为成千上万）、概率支付等。

6.金额隐藏技术

以下工作由亚当·拜克首次在Bitcointalk上的帖子《同态值比特币》中提出。

①佩德森的承诺。CT（密码学承诺）的基础密码学工具是佩德森的承诺。

承诺场景让你把一段数据作为私密保存，但是要承诺它，使你以后

不能改变该数据。一个简单的承诺场景用哈希函数构建如下：

$$\text{承诺} = \text{SHA256}(\text{盲化因子} \parallel \text{数据}) \quad (\text{式 3-1})$$

如果你仅告诉别人承诺，别人没法确定你承诺了什么数据。但你后来揭露了盲化因子和数据，别人可以运行该哈希函数来验证是否与你之前的承诺相匹配。盲化因子必须存在，否则别人可以试图猜测数据。如果你的数据比较少而简单，猜测成功的可能性比较大。

佩德森承诺与以上场景中的承诺类似，但是附加一个特性：承诺可以相加，多个承诺的总和等于数据总和的承诺（盲化因子的集合即盲化因子总和）：

$$C(\text{BF1}, \text{data1}) + C(\text{BF2}, \text{data2}) = C(\text{BF1} + \text{BF2}, \text{data1} + \text{data2}) \quad (\text{式 3-2})$$

$$C(\text{BF1}, \text{data1}) - C(\text{BF1}, \text{data1}) = 0 \quad (\text{式 3-3})$$

换句话说，加法律 and 交换律适用于承诺。

$$\text{If data_n} = \{1, 1, 2\} \text{ and BF_n} = \{5, 10, 15\} \text{ then: } C(\text{BF1}, \text{data1}) + C(\text{BF2}, \text{data2}) - C(\text{BF3}, \text{data3}) = 0 \quad (\text{式 3-4})$$

我们用椭圆曲线点来构建具体的佩德森承诺（读者无须理解椭圆曲线密码学体系，把它当成黑盒行为来了解就可以了）。通常，ECC公钥由私钥 x 乘基点 G 生成。

$$\text{PUB} = xG \quad (\text{式 3-5})$$

结果保存为33字节的数组。ECC公钥遵守以前描述过的加法同态性：

$$\text{PUB1} + \text{PUB2} = [\text{x1} + \text{x2} \pmod{n}] G \quad (\text{式 } 3-6)$$

(以上特性被BIP32分层确定性钱包用来允许第三方生成新的比特币地址。)

由于佩德森承诺的额外基点（称之H点）生成方法，因而没人知道H对G的离散对数（反之亦然），即没人知道x，且 $xG=H$ 。我们使用G哈希来选择H：

$$H = \text{to_point} \{ \text{SHA256} [\text{ENCODE} (G)] \} \quad (\text{式 } 3-7)$$

这里to_point把输入当成椭圆曲线上某个点的x值，并且计算出y值。给定两个基点我们能构建如下承诺场景：

$$\text{承诺} = xG + aH \quad (\text{式 } 3-8)$$

这里x是私密盲化因子，a是我们要承诺的金额，你可以用加法交换律验证加法同态承诺场景中的相关关系。

佩德森承诺是信息理论上的隐私，你看到的所有承诺，总能找到一些盲化因子，可以和任意金额一起匹配该承诺。如果你的盲化因子是真随机，那么拥有无穷计算力的攻击者都不能分辨你承诺的金额。这种承诺无法被假冒，没法计算出任意其他能被验证的承诺。如果你做到，这就意味着你能找到两个基点相对于彼此的离散对数，意味着承诺椭圆曲线公钥体系被破解。

②佩德森承诺应用。

利用该工具，我们替换比特币交易中的8字节金额为32字节佩德森承诺。如果一个交易的发送人认真选择他们的盲化因子，以便正确相加,然后人们还能通过承诺相加为0来验证该交易。

$$(In1 + In2 + In3 + plaintext_input_amount \times H \cdots) - (Out1 + Out2 + Out3 + \cdots fees \times H) = 0 \quad (\text{式 3-9})$$

以上公式需要明确的交易费用，在实际交易中，这点没有问题。生成承诺和承诺验证非常简单，不幸的是，如果没有附加的措施这个场景是不安全的。

问题在于该群是循环群。加法要mod P（一个256位的质数，用于定义群的秩），结果大数的加法会“溢出”，从而像个负数金额，因而当有些输出金额为负数时，承诺加起来为0的特点依然存在，导致可凭空创造5个比特币。

$$(1 + 1) - (-5 + 7) = 0 \quad (\text{式 3-10})$$

以上式子可以被解释成“有人花了2个比特币，得到-5个比特币和7个比特币”。为了防止产生这种情况，交易中有多输出的时候，我们必须证明每个承诺输出金额都在允许范围（如[0, 2~64]）内且没有溢出。

我们可以公开金额和盲化因子，以便其他人能检查，但是这样一来就损失了所有隐私。因而，我们要证明承诺的金额在允许范围内，除此之外不透露任何信息。我们可以使用类似于Schoenmakers二元分解的技术来解决此问题，但是在此基础上进行了许多优化（包括不使用二元）。

我们从基本的EC签名开始，如果生成了一个签名，签名的消息是

公钥的哈希，该签名证明签名者知道私钥，即公钥对于某些基点的离散对数。

对于一个类似公钥的 $P=xG+aH$ ，因为基点 H 的存在，没有人知道 P 对于基点 G 的离散对数，因为没人知道 x 使得 $xG=H$ ，除非 a 为0。如果 a 为0，则 $P=xG$ ，离散对数恰好是 x ，有人会为该公钥签名。

把承诺当成公钥，对承诺的哈希值签名，通过这种方法，某个佩德森承诺可以被证明是对0值的承诺。在签名中使用公钥用于防止把签名设置成任意值并且破解出承诺。签名使用的私钥正是盲化因子。

更进一步，假定我想证明 C 是对金额1的承诺，但不告诉你盲化因子，你能做的就是计算：

$$C' = C - 1H \quad (\text{式 } 3-11)$$

然后向我要公钥 C' 的签名（相对于基点 G 的签名），如果我能做到，则 C 一定是对金额1的承诺（否则我就破解了EC离散对数的安全性）。

③环签名。

为了避免给出金额，我们还需要另一个密码学技术：环签名。环签名是当存在两个（或多个）公钥的签名场景时，签名证明签名者知道至少一个公钥的离散对数。使用环签名，我们可以构建另一个场景。我证明一个承诺是对金额0或金额1的承诺，我们叫这种场景为“或证明”。

首先，我给你 C ，你计算 C' ： $C' = C - 1H$

然后我提供 $\{C, C'\}$ 上的环签名。

如果C是对金额1的承诺，则我不知道它的离散对数，但是C'成为金额0的承诺，我知道它的离散对数（就是盲化因子）。如果C是对金额0的承诺，我知道它的离散对数；C'是对金额1的承诺时，我不知道离散对数。如果这是一个对任意其他金额的承诺，没有一个结果为金额0，因而我没法签名。

以上机制对任何数字都有效，只需把金额进行合适的预处理再放到环中，或者超过2个数字。

假定我想证明C在范围[0,32)之中，现在我们有一个或证明，想象我发送给你一个承诺集合，每个承诺都有个或证明：

C1 is 0 or 1 C2 is 0 or 2 C3 is 0 or 4 C4 is 0 or 8 C5 is 0 or 16

我为C1—C5选择了正确的盲化因子，能使得 $C1 + C2 + C3 + C4 + C5 = C$ 。我建立了一些有效的二进制数，和一个只能在区间[0,32)内的5位数。

众多优化手段可以让证明过程更有效。

首先，我们提出一个新的、更有效的环签名方法——Borromean环签名，它仅要求每个公钥32字节，再加上能被其他不同环所共享的32字节。与以前提出的构建方式相比，该环签名能达到两倍效率。

CT金额并非直接表述金额，而是使用十进制浮点数来表示，每个数字要与以10为基数的指数相乘，这意味着如果在基数10之前有较少重要数字，你能用小容量证据来证明大金额。比如：11.2345和0.0112345可以有相同大小的证明，即使两个数相差一千倍。

还有一个非隐私的发送“最小金额”。如果用户愿意泄露一些最小金额信息（最小金额信息将对外公开），那么就允许更小的证据覆盖更大范围的金额，并且当使用指数时还允许最小重要数字非零。用交易中第

一个金额减少最小的金额，然后证明该值非负。

其次，浮点尾数用四进制编码而不用二进制，因为可以减少要发送的承诺的数值，使得签名数据大小与二进制相当。对最后的尾数数字的承诺可以跳过，从前向后对已经证明的金额创建承诺，其他数字也一样。

最后，通过在证明中小心使用非随机化签名，对于币的接收者（由于带接收者公钥的ECDH密钥协议，他与发送者共享一个私钥）来说，“重绕”证据并且用它提取发送者发送的消息是可能的。该消息大小为证据大小的80%。我们使用该原理向接收者提供金额和盲化因子，但是也可以用来存储编号或撤款地址等信息。

三、闪电网络

闪电网络（The Lightning Network）是一个去中心化的系统。闪电网络的卓越之处在于，无须信任对方以及第三方即可实现实时的、海量的交易。

（一）闪电网络的起源

近年来，随着比特币的蓬勃发展，比特币交易数量越来越多，而单个区块体积有1MB的最大值限制，因此区块空余空间显得越来越小。如图3-5所示，区块体积中位数在2015年里得到了翻番，从1月的292KB（千字节）快速增长至12月的749KB。

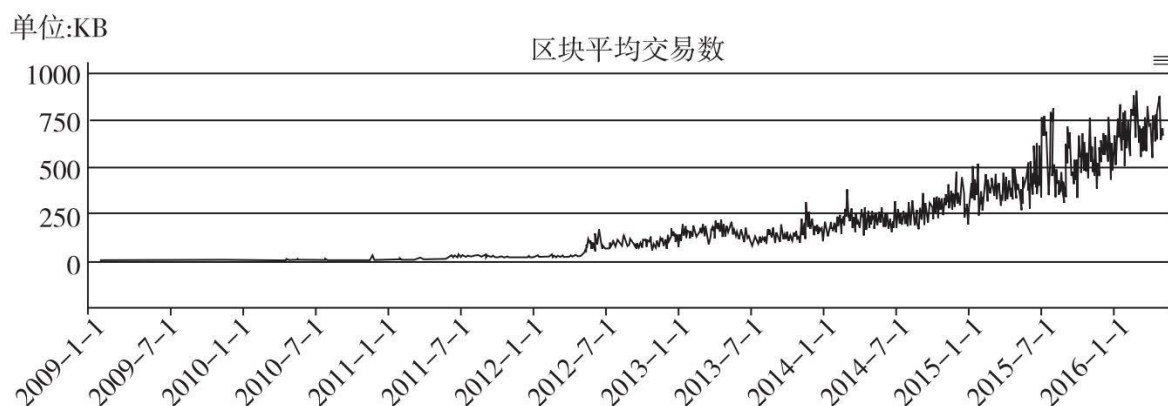


图3-5 比特币区块体积大小

数据来源：区块元blockmeta.com

扩容问题在2015年得到了充分的重视与讨论，在2015年6月左右陆续推出了诸多扩容方案，代表有BIP100、BIP101、BIP102、BIP103、BIP109、BIP248等若干方案（见表3-2）。

表3-2 区块扩容方案表

编号	扩容方案
BIP100	由矿工们进行投票，将新的区块建议上限值写在 Coinbase 交易中，新的值在当前的基础上有 20% 的上下浮动空间。全网 80% 的算力参与可激活新的大小。
BIP101	自 2016 年起，立即提升限制值为 8MB，然后每两年翻番并持续至 2036 年，届时区块体积限制值为 8.2GB。
BIP102	体积限制一次性地从 1MB 提升至 2MB。

编号	扩容方案
BIP103	每个特定周期增长 4.4%，折合年增长率为 17.7%，直至 2063 年 7 月，届时体积约为 1.4GB。
BIP109	全网 75% 的算力可激活，体积限制提升至 2MB。
BIP248	2016 年将体积限制提升至 2MB，2018 年提升至 4MB，2020 年提升至 8MB。

虽然提出各种方案，但基本可以划分为两类：长期规则派与短期搁置派。长期派偏理想、规则型，一口气敲定便不再折腾，典型代表是BIP101/103，设定一个增长规则，便不再调整。短期派则认为未来不可预测，固定的规则过于简单暴力，希望设置一个短期数年方案暂时先避开，搁置至未来解决，代表为BIP100，但由于投票过程复杂，后简化为BIP102/109等，而BIP248则一口推迟至2020年，近几年就简单采取翻番增长。

自2015年6月至今，经过了大半年来大范围的反复讨论，目前长期规则派基本完败。2015年12月比特币香港扩容会议由Pieter Wuille提出了隔离见证（Segregated Witness）之后，扩容问题甚至已经简化为仅升级至2MB，但陷入了关于实施时间点的争论之中。

一个看似简单的扩容技术问题，却引发比特币社区花了大半年时间，开了数次全球技术会议、私下打了无数回口水仗，却依然未有明确定论。其背后深刻的原因是，区块限制值上调是无法真正解决比特币扩容问题的。

（二）扩容问题

总的来说，根据对比特币网络的理解，有两个划分：清算系统和现金系统。

1.清算系统

比特币区块链是全球的、分布式的、有限容量的且代价昂贵的系统。每一笔交易的价值含量是不一样的，当块容量不够用时，我们应该保障高价值的交易进块。高价值的交易有意愿、有能力支付足够高的网络手续费，从而获得足够高的优先级进块。

随着比特币的繁荣，交易数量会越来越大，有限的块容量会使低价

值的交易（例如发送1分钱）永远无法进块，因为低价值的交易不可能支付高网络手续费。进而，网络退化为清算系统，低价值含量交易被赶出，这些交易由第三方记账系统进行代替完成。

在闪电网络出现之前，第三方记账系统主要是链外钱包提供商。用户信任某第三方钱包平台，把比特币存入其中，同一平台用户之间转账仅带来账户余额变更，并不会产生比特币交易。

2.现金系统

现金系统意味着所有交易均应该进入区块，那么当块容量不够用时，则应该及时调整块体积限制，对系统进行扩容。短时间可能发生交易入块堵塞，但长期来看所有交易应该均可以入块，人人都享有比特币系统带来的巨大便利和优势。

3.扩容大小的选择

我们进行一个简单的估算，假设每个交易大小为512字节，手续费单位为0.0004/KB（见表3-3）。

表3-3 区块未扩容方案表

交易/秒	单个块体积	块手续费	全年块体积
1	0.3 MB	0.12 BTC	15 GB
3	0.9 MB	0.36 BTC	47 GB

交易/秒	单个块体积	块手续费	全年块体积
10	3 MB	1.2 BTC	150 GB
100	30 MB	12 BTC	1.5 TB
1000	300 MB	120 BTC	15 TB
10000	3 GB	1200 BTC	150 TB
100000	30 GB	12000 BTC	1500 TB

根据VISA在2015年的记录，全年共产生92064百万笔支付交易，折合比特币网络数据（见表3-4）。

表3-4 区块扩容方案表

交易/秒	单个块体积	块手续费	全年块体积
2920	897 MB	358 BTC	47 TB（太拉字节）

若提高区块体积限制至30MB，最大的问题不是CPU计算能力瓶颈，而是块的传播与存储。

30MB的块可能会导致全网孤块率和空块率大幅上升，一年产出1.5TB的区块链数据也超出大部分节点机器的硬盘容量。基于这1.5TB的数据，区块链浏览器、钱包服务商等则可能膨胀10倍达到15TB。这对于目前来说，已经远超普通机器/数据库的磁盘容量。

诚然，这些数据对于中性化的系统而言，并不具有多么大的挑战性，但对于一个全球分布式系统而言，则非常具有挑战性，会极大削弱节点数量，提高开发接入门槛，使比特币变得中心化。

扩容争论的最后，还是倾向于2MB，使升级过程更加可控一些，风险更低一些。

（三）微支付通道

闪电网络在一片扩容的吵闹声中于2015年7月发出了首篇论文。在介绍闪电之前，我们先介绍一下微支付通道（Micro-Payments Channel）。

微支付通道概念于2012年首次被提出，是解决小额度、高频次支付场景的方案，目的在于缩减支付的交易数量，使高频、小额支付成为可能。下面我们先研究一下微支付通道的原理。

假设爱丽丝为消费者，鲍伯为一家视频网站。爱丽丝非常喜欢去鲍伯网站看电影，看一部电影需要支付0.1BTC（比特币），那么爱丽丝看了10部电影就需要支付10次0.1BTC，共计1BTC并发出10笔交易。而采用微支付通道就会缩减至两笔，或者说任何多次的交易均会缩减至两笔，只要总金额不超过存入通道的额度即可。

通道（Channel）的建立以及更新过程如下。

①爱丽丝支付1BTC至一个多重签名地址，签名采用2/2方式，我们把该交易称为FTX(Fund Tx)。爱丽丝生成该交易后，并不广播。

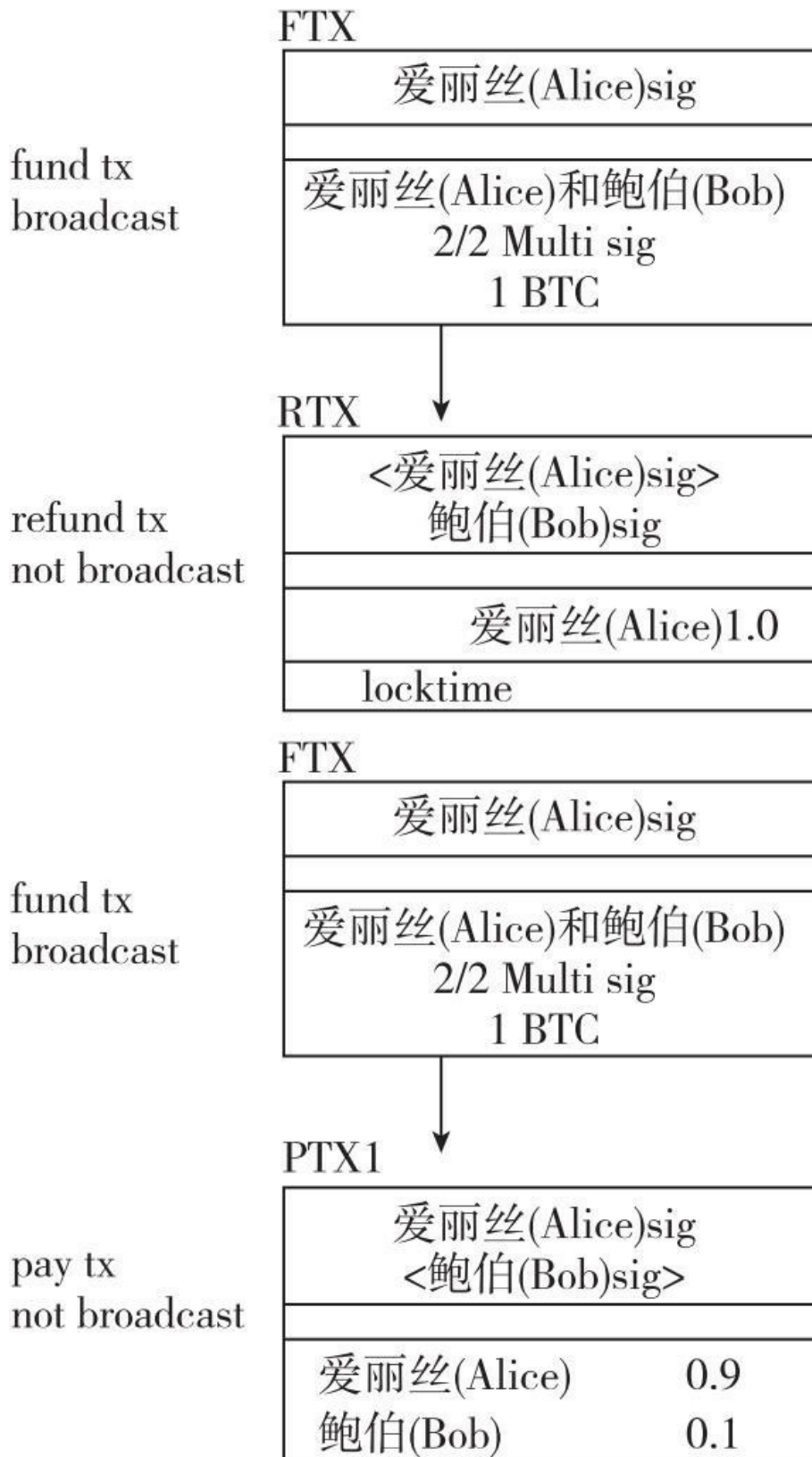


图3-6 微支付交易结构

②爱丽丝再构造一个赎回交易，称之为RTX(Refund Tx)。其输入为交易FTX的输出，输出为爱丽丝自己。同时，该交易有Locktime锁定期，所以N天之后才会生效，才可以进块。

③爱丽丝把构造好的空RTX给鲍伯，并让鲍伯进行签名。

④爱丽丝拿到带有鲍伯签名的交易RTX后，广播出FTX。此时的交易结构如图3-6所示，图中带有尖括号的签名表示待填入。

⑤爱丽丝再看了一部电影，那么她需要再支付0.1BTC给鲍伯。于是，爱丽丝构造另一笔交易PTX2：输入依然是交易FTX；输出为两个地址，其中爱丽丝为0.8BTC，鲍伯为0.2BTC。爱丽丝对该交易签名，并将交易和她的签名给鲍伯（图3-7）。

⑥鲍伯可以随时签名并广播交易PTX2，当然，他依然可以广播交易PTX1。作为一名理性经济人，鲍伯必然总是广播自己收益最大的那笔交易，也就是当前的PTX2。在目前总是爱丽丝付款的情况下，鲍伯总是乐于广播最后一个交易。

⑦当鲍伯广播出最后一笔交易PTX_n时，则意味着通道关闭，合作结束。鲍伯需要在交易RTX锁定期结束前关闭通道，否则意味着爱丽丝可以在交易RTX解锁后拿回她所有的币。

上述，就是微支付通道建立、更新与关闭过程。在一个完整的过程中，有且仅有两笔交易广播至链上，

同时双方均无须信任对方，任何一方也无法侵害另一方的利益。在更新过程中双方只是交换交易和签名数据，并无交易广播至链上，那么意味着在存入额度范围内，

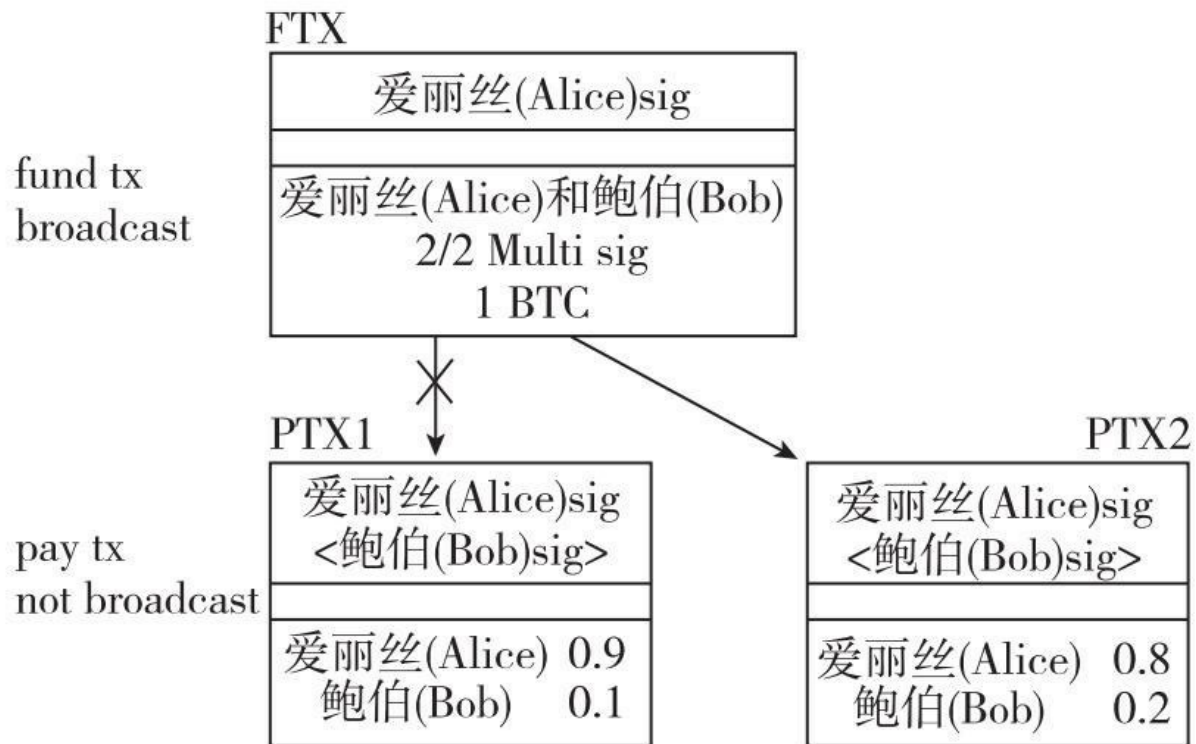


图3-7 微支付交易广播收益最大化的那笔交易

可以创造出无数笔交易。不仅通道内的更新次数不受限制，频率也可以达到非常高，只要系统允许，目前硬件条件可以轻松达到每秒数千笔。

在特定场景下，微支付通道拥有着巨大优势，让小额高频支付成为可能。但它存在一个巨大制约：币在通道中的流向是单向的。在上述例子中，币仅能从爱丽丝流至鲍伯。

（四）闪电网络交易合约

微支付通道解决了合并交易的问题，但并没有解决撤销上个交易的问题，利用“理性经济人”和单向流动来达到撤销上个交易目的，并不是真正的撤销。若交易可以撤销，则币可双向流动。

闪电网络是基于微支付通道演进而来，创造性地设计出了两种类型

的交易合约：序列到期可撤销合约RSMC（Revocable Sequence Maturity Contract），哈希时间锁定合约HTLC（Hashed Timelock Contract）。

RSMC解决了通道中币单向流动问题，HTLC解决了币跨节点传递的问题。这两个类型的交易组合构成了闪电网络。

1.RSMC创建

我们先来创建一个序列到期可撤销合约（RSMC）。爱丽丝和鲍伯是合作方，经常有比特币往来，所以他们决定各拿出0.5BTC放入通道中，便于业务往来。

RSMC交易结构（图3-8）的下方，左侧为爱丽丝的视角，右侧为鲍伯的视角。中间Funding Tx为共同可见；C1a和RD1a为爱丽丝持有；C1b和RD1b为鲍伯持有。交易图中带有尖括号的签名表示待填入。

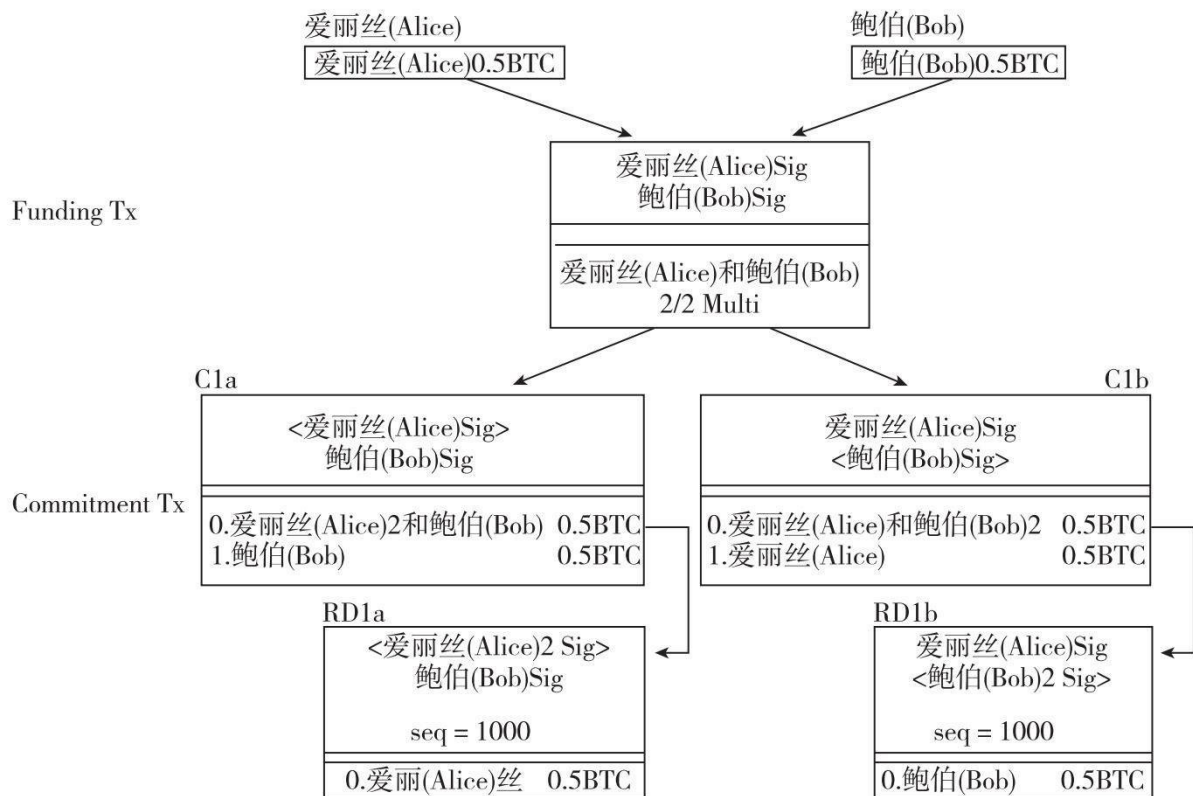


图3-8 RSMC交易的结构图

①双方各拿出0.5BTC，构建Funding Tx，输出为爱丽丝和鲍伯的2/2多重签名。此时，Funding Tx未签名，更不广播。

②爱丽丝构造Commitment Tx：C1a和RD1a，并交给鲍伯签名。C1a的第一个输出为多重签名地址，爱丽丝的另一把私钥爱丽丝2和鲍伯的2/2多重签名，第二个输出为鲍伯0.5BTC。

③RD1a为C1a第一个输出的花费交易，输出给爱丽丝0.5BTC，但此类型交易带有sequence，作用是阻止当前交易进块，只有前向交易有1000个sequence确认时才能进块。

④鲍伯构造Commitment Tx：C1b和RD1b，并交给爱丽丝签名。结构与C1a、RD1a是对称关系。

⑤鲍伯对C1a和RD1a进行签名，并将签名给爱丽丝；同理，爱丽丝对C1b和RD1b签名，完成后给鲍伯。此时，由于并未对Funding Tx进行签名，任何一方均无法作恶，任何一方也不会有任何损失。

⑥双方均完成对Commitment Tx的签名并交换后，各自再对Funding Tx进行签名，并交换。此时，Funding Tx是完整的交易，广播之。

上述过程以及结构图的描述，就是创建RSMC的全部过程。

C1a和C1b两笔交易花费的是同一个输出，故他们两个交易只有一个能进块。若爱丽丝广播C1a，则鲍伯立即拿到0.5BTC（C1a的第二个输出），而爱丽丝需要等C1a得到1000个确认，才能通过RD1a的输出拿到0.5BTC。另一方，若鲍伯广播C1b，则爱丽丝立即拿到0.5BTC，鲍伯等待C1b得到1000个确认，才能通过RD1b拿到0.5BTC。也就是说，单方广播交易终止合约的那一方会延迟拿到币，而另一方则立即拿币。

2.交易更新

爱丽丝和鲍伯各自有0.5BTC的余额，此时爱丽丝从鲍伯处购买了一件商品，价格为0.1BTC，那么余额应该变为爱丽丝0.4BTC，鲍伯0.6BTC。于是创建新的Commitment Tx，对于爱丽丝来说是C2a和RD2a，对于鲍伯来说是C2b和RD2b，过程与上面类似（图3-9）。

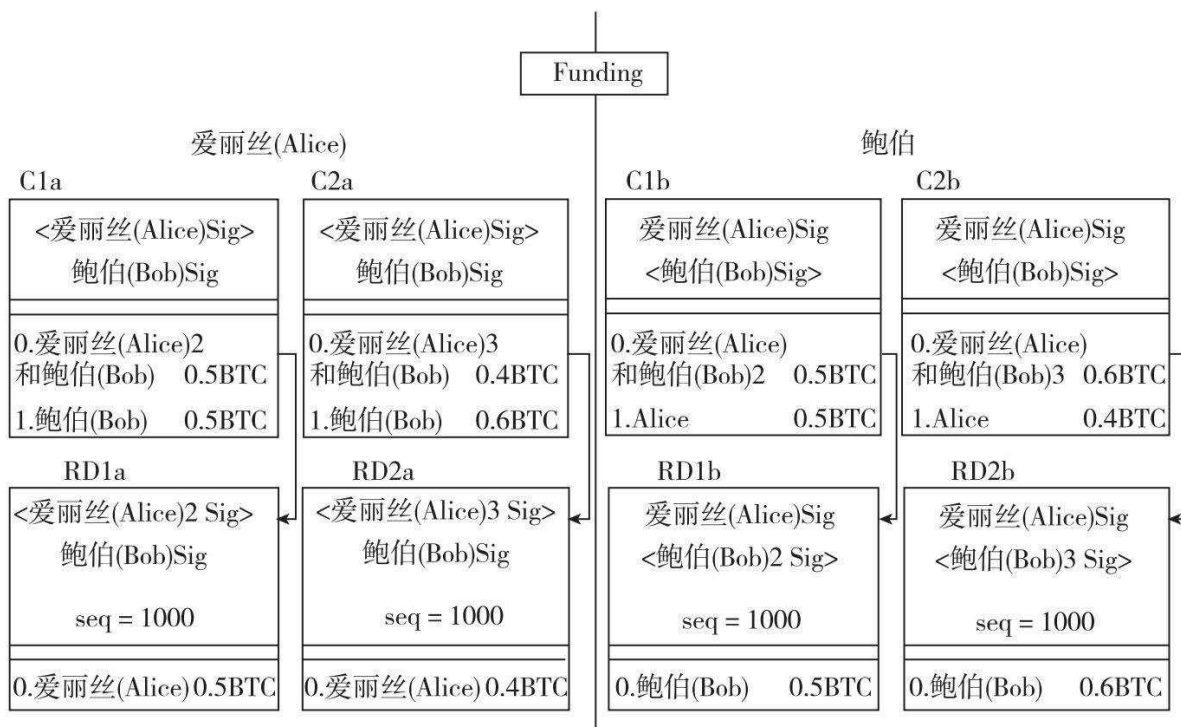


图3-9 交易更新时的交易结构

此时两个状态均是有效的，那么最核心的问题来了：如何才能彻底废弃C1a和C1b呢？

RSMC采用了一个非常巧妙的方法：在C1a的第一个输出中，采用了爱丽丝2和鲍伯的多重签名，爱丽丝将爱丽丝2的私钥交给鲍伯，即表示爱丽丝放弃C1a，承认C2a（图3-10）。

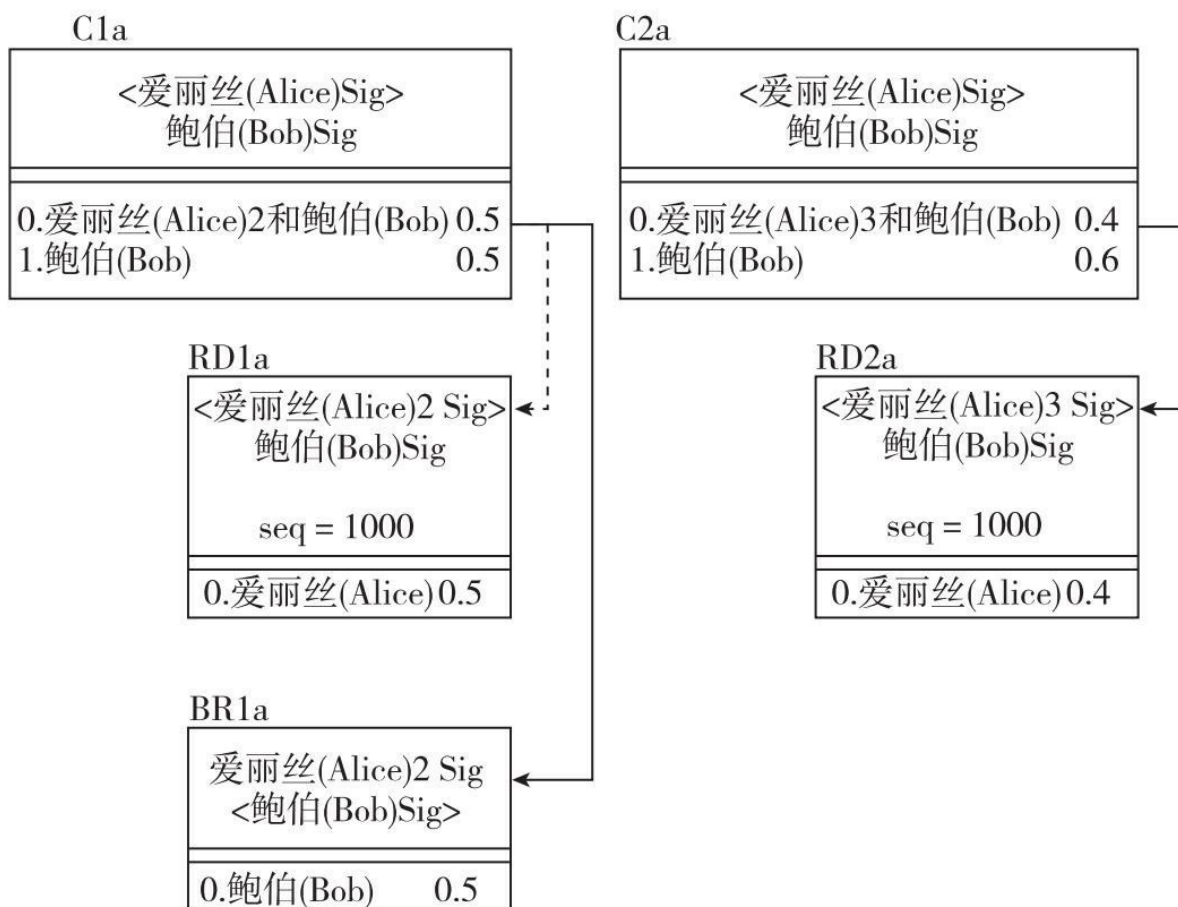


图3-10 交易更新时的多重签名

爱丽丝交出爱丽丝2的私钥给鲍伯，那么鲍伯就可以修改RD1a的输出给他自己，形成新的交易BR1a。若爱丽丝破坏合约，在存在C2a的情况下依然广播出C1a，那么爱丽丝受到的惩罚就是失去她全部的币。爱丽丝交出爱丽丝2的私钥，或者对交易BR1a进行签名，两者是等同的，都是对C1a的放弃。

反之亦然，鲍伯交出鲍伯2的私钥给爱丽丝即意味放弃C1b，而仅能认可C2b。

引入sequence的目的是，阻止后续交易进块（RD1a），给出一个实施惩罚窗口期，当发现对方破坏合约时，可以有1000个块确认的时间去实施惩罚交易，即广播BR1a代替RD1a。若错过1000个块时间窗口，则

无法再实施惩罚了（RD1a进块了）。

3.交易关闭

关闭RSMC，直接按照最终的余额构造出一个Commitment TX即可。例如，输出为爱丽丝0.1BTC，鲍伯0.9BTC，无需再设置多重签名，构造惩罚交易等。

4.中转交易

爱丽丝想要支付0.5BTC给鲍伯，但她并没有一个渠道来和他进行交易。幸运的是，她和查理有一个交易渠道，而查理正好和鲍伯有一个交易渠道。这样爱丽丝就能借助查理的交易渠道，通过哈希时间锁定合约（HTLC）来和鲍伯进行交易了（图3-11）。

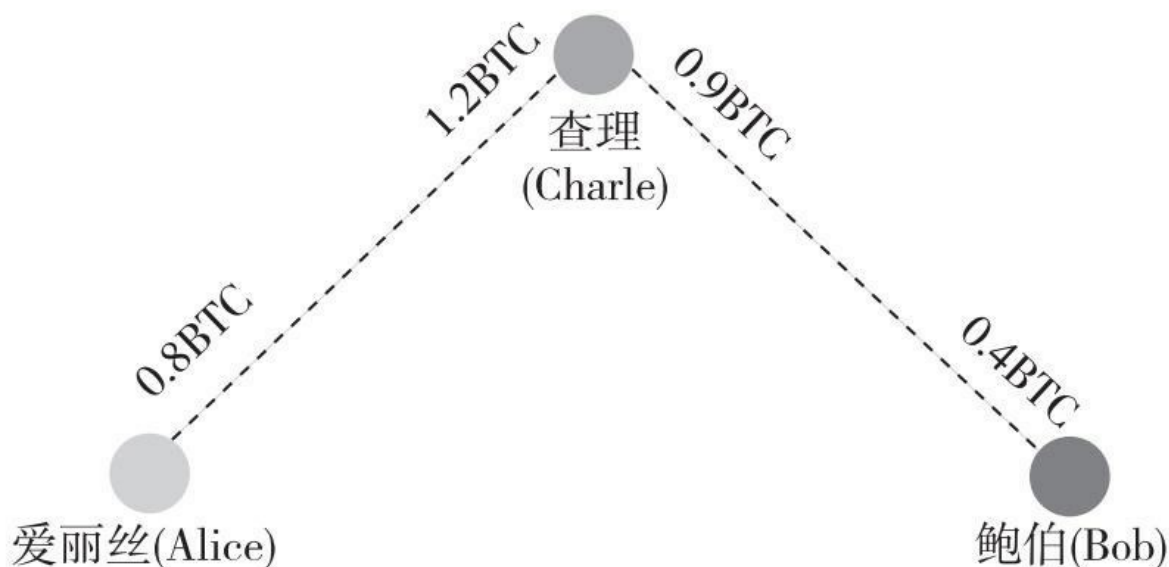


图3-11 中转交易示意图

为了完成这次交易，爱丽丝就会给鲍伯发短信说：“嘿！我要给你付笔款。”这时鲍伯将收到一个随机数字（R），接着鲍伯便会回一个被哈希的数字（H）（你可以认为被哈希的数字H是随机数字R的一种加密

形式)给爱丽丝。然后爱丽丝的钱包紧接着就会联系查理说:“嘿,查理。如果你给我生成(H)的未加密值(R),那么我就同意更新我们渠道的支付分配,这样你得到的就会比0.5BTC多一点,我得的比0.5BTC少一点。”尽管查理并不知道R,但他也会同意。之后查理便会去找鲍伯说:“嘿,鲍伯。如果你给我那个能生成H的未加密的值R,我将同意更新我们渠道的支付分配,这样你得到的会比0.5BTC多一点,我得到的比0.5BTC少一点。”

因为R就是从鲍伯这里生成的,所以他肯定知道。接着他马上将R告诉查理,并更新了其渠道的支付分配。然后查理将R告诉给了爱丽丝之后也更新他们的渠道,最后交易完成,爱丽丝以脱链的形式付给鲍伯0.5BTC。

5.总结

RSMC通过巧妙地设置Commitment TX的多重签名输出,以及sequence的延迟进块形成惩罚窗口期,解决了在微支付通道中的币单向流动问题。

(五) 闪电网络面临的问题

闪电网络的最初设想为一个中心辐射型网络(图3-12)。你的钱包将会连接到一个“支付中转站”,由于各种支付渠道彼此之间都保持畅通,爱丽丝有一个和中转站A相通的渠道,而鲍伯也有一个和中转站B相通的渠道,爱丽丝只需通过一两个中转站的跳跃就能直接和鲍伯交易了。

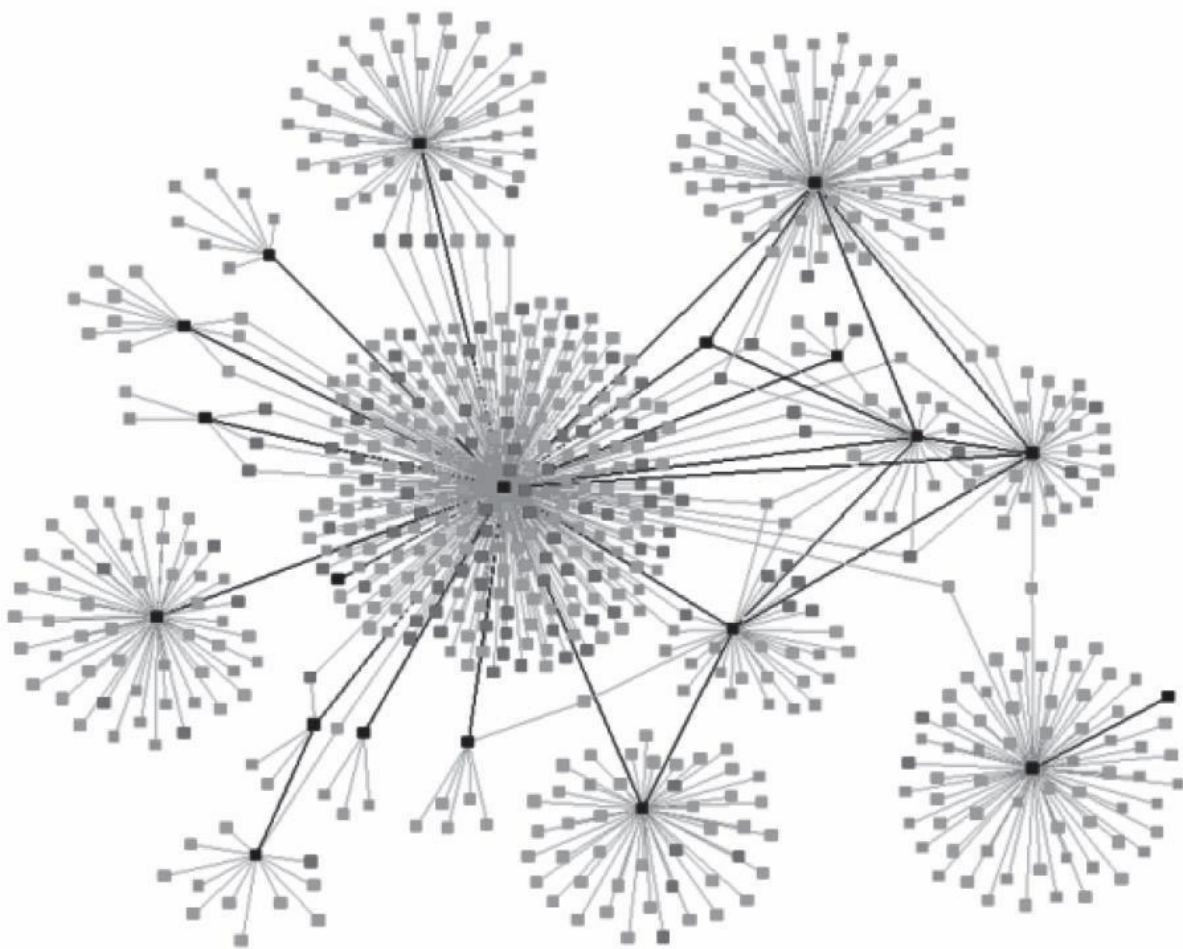


图3-12 中心辐射型网络

如果能有成百上千个中转站（小额支付中心），那么这个网络拓扑结构就能完美运行。但是，若是只有少数几个大型中转站，那么这个网络的去中心化就会受到损害，变成另一个VISA卡、万事达卡或者美国运通。

1.中转站的中心化风险

要精确地预测出存在于网络均衡中的中转站的数量是完全不可能的，但是由于众所周知的马太效应，这个数字会逐渐变小，而不是变大。然而不可否认的是，在开源项目中，任何人都可以在上面运行一个

支付中转站（至少在政府部门决定监管之前），只是支付中转站运行的高成本就像是给进入者们设置了一道坚固的壁垒，从而产生了中心化压力。

为什么建立支付中转站需要高成本？让我们回到查理扮演“交易中转站”的那个例子。回想一下，爱丽丝需要通过查理把比特币付给鲍伯，所以查理不得不在更新他和爱丽丝的分配渠道之前就更新他与鲍伯的分配渠道（付给鲍伯的多，自己得到的要少）。也就是说，查理在得到鲍伯的0.5BTC之前，就得先付钱给爱丽丝。

这意味着如果查理想要成为一个支付中转站，那他自己必须在与“客户”共有的渠道里存足够多的比特币，这样才能促成这些“客户”的脱链交易。如果查理没有预存至少0.5BTC到鲍伯的渠道里，那么这笔交易就不能做成。

现在，虽然查理仍保留这些比特币百分之百的控制权，但是这笔钱至少还是需要放在那些渠道里，以便促成那些链外支付，因而资金的沉淀成本非常高昂。所以，要运行一个支付中转站还是需要真金实银的投入，最起码在刚开始之前就需要准备足够的预存款。

那么，一个支付中转站应该给每个渠道存入多少预存款呢？如果一个比特币是500美元的话，那么你想要运行一个服务100人的支付中转站，需要50000美元的资产来启动它。

因此，如果某天闪电网络最终演变为中转站辐射型拓扑网络，那么中心化就是它最大的隐患。

2.点对点的路径交易

闪电网络是否有比中转站辐射型更好的模式？目前已经有很多规避支付中转站的设想，开发者尝试创造出更多去中心化、有组织的钱包对

钱包的路径。

试想一下，如果爱丽丝想要买一杯咖啡，在此之前，她的钱包会用相同的技术在网络中通过其他节点找到一个路径来支付这杯咖啡。如果钱包找不到任何一个节点，那么它将与咖啡店打开一个新的支付渠道来完成这笔交易，然后留着这个渠道以便日后再用。理论上爱丽丝的钱包能够维持数十个开放的渠道。

如果有人每次在尝试支付时都不能找到一个渠道，那么新的渠道将会被打开，长此以往，用户间的一些有组织的渠道路径就会形成（图3-13）。

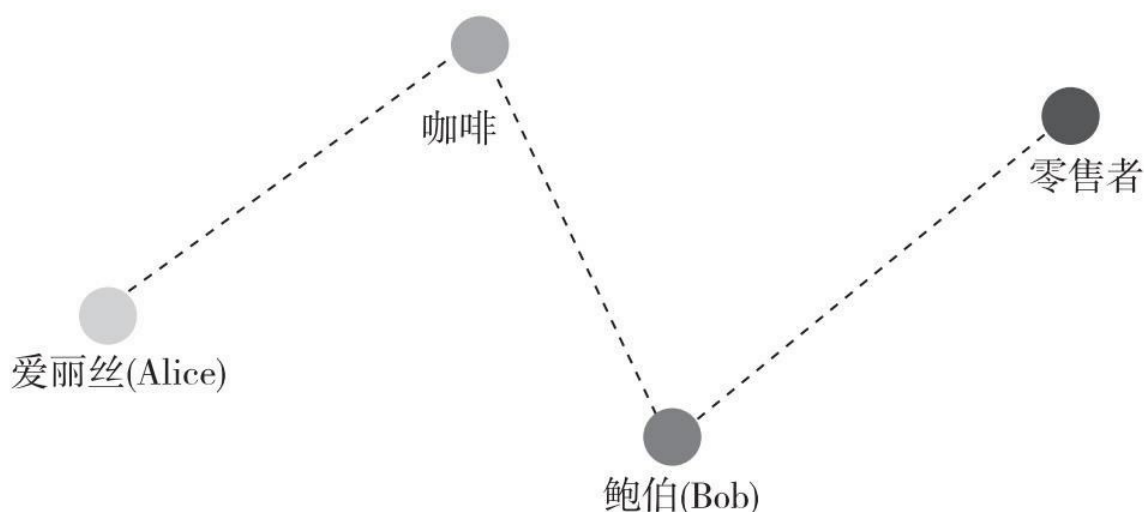


图3-13 点对点的路径交易示意图

从图3-13我们可以看到，爱丽丝在离开咖啡店后仍保持其支付渠道的开放。鲍伯最近去了咖啡店后也保持其支付渠道的开放，而且他还从商店里买了一条新领带，这个支付渠道也是处于开放状态。

在这个例子中，爱丽丝不仅可以将比特币以链外的形式给鲍伯，还可以通过已形成的有组织的路径将比特币付给商店老板。这可以解决闪电网络中心化的问题。但在具体应用中，很难找到从爱丽丝到商店并通

过咖啡店和鲍伯的支付路径。

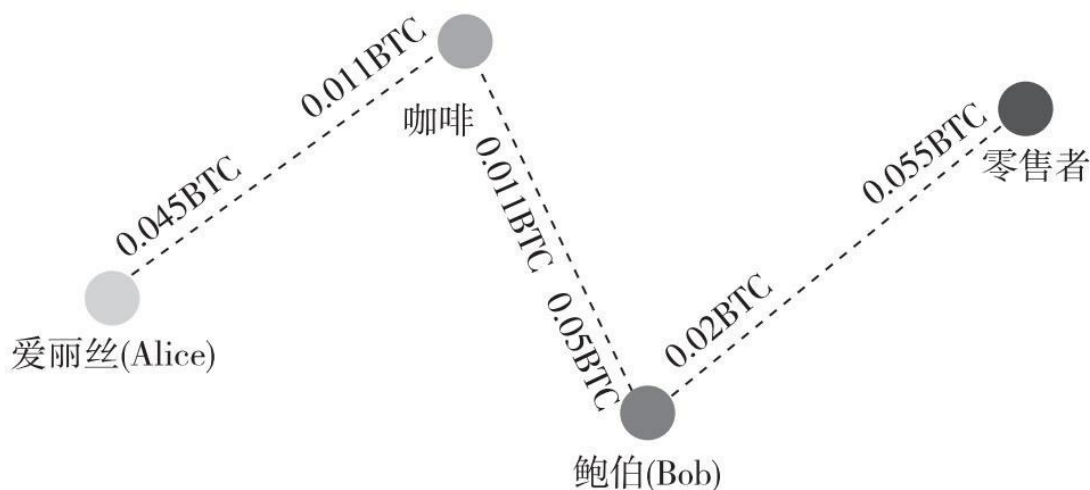


图3-14 点对点交易的支付路径

爱丽丝和鲍伯都要花0.011BTC来买一杯咖啡（约5美元），这就是为什么咖啡店在爱丽丝和鲍伯的渠道中都有0.011BTC（图3-14）。对爱丽丝来说，不管她是想把钱给鲍伯还是商店老板，咖啡店老板都需要更新他和鲍伯的支付分配渠道。咖啡店老板自己得到的少（从爱丽丝想要付的钱中），鲍伯从中得到的多。但是注意一下，咖啡店老板在和鲍伯的渠道中只有0.011BTC（约5美元），也就是说爱丽丝最多只能付给鲍伯或是商店老板5美元。如果她想要付更多的钱，那她就需要重新开一个渠道。

当人们以不同金额买不同的东西时，这种类型的数值不对称性就很有可能会频繁发生。从一个节点到另一个节点的路径很容易被找到，但是每一次找到正确数值的跳跃路径则是最困难的部分。

3.路径交易造成更多的链上交易

设想一下，要是爱丽丝的钱包不能从商店那里找到一条她想要数额的路径时，她是怎样开启一条新的渠道的。据估算，在给定的时间内你

钱包中的比特币有绝大部分会留在渠道中。那么爱丽丝的钱包哪里还有比特币来和商店开一个新的渠道呢？好，如果它不得不关闭现存的渠道之一，那么当你的钱包在交易时不能找到一条路径的过程将是这样：①关闭现有的一条渠道完成链上交易。②和收款人开启一条新的渠道完成链上交易。

这两笔链上交易中还只有一笔付款，要是有一笔大交易无法找到一条路径（因此不得不关闭一个旧的渠道来打开一条新的渠道），很多的预存款都将被浪费掉。如果有超过50%的交易找不到路径，闪电网络实际上会促成更多的链上交易，而不是即时的链外交易。

4.路径交易时，发送者和接收者需要同时在线

人们即便是使用桌面上的钱包，也不会让它24小时都开启。他们在不用钱包的时候就会关闭程序，盖上笔记本电脑的盖子，关掉电脑等。除此之外，很多人的手机钱包都是休眠状态，不会时刻保持上线状态。因此，99%的预期用户都不会参与路径付款。

在哈希时间锁定合约（HTLC）的例子中，爱丽丝的钱包联系鲍伯的钱包，并问他要一个哈希化的随机数字（R）。鲍伯需要在线才能将那个数字给她。而在比特币目前的使用中，发送者和接收者是不需要同时在线的。

参考资料

[1]<http://8btc.com/article-2002-1.html>

[2]<http://www.bitabc.com/?id=169>

[3]<http://www.8btc.com/merkling-in-ethereum>

[4]<http://8btc.com/thread-23806-1-8.html>

[5] <http://8btc.com/article-1790-1.html>

[6] <http://www.8btc.com/confidential>

[7] <http://www.8btc.com/elements>

[8] <https://www.elementsproject.org/elements/deterministic-pegs/>

[9] <https://www.elementsproject.org/sidechains.pdf>

[10] <https://github.com/ElementsProject>

[11] https://github.com/Blockstream/borromean_paper/raw/master/borromean_paper.pdf

[12] https://people.xiph.org/~greg/confidential_values.txt

[13] <https://bitcointalk.org/index.php?topic=305791.0>

[14] <https://www.elementsproject.org/elements/relative-lock-time/>

[18] 本章《简单支付验证》部分由海滨完成，《侧链》部分由申屠青春完成，《闪电网络》部分由潘志彪完成。

申屠青春，深圳银链科技CEO，深圳大学ATR国防科技重点实验室博士。

潘志彪，现任比特大陆软件研发总监，BTC.COM团队负责人。前币付宝CTO、联合创始人。中国比特币行业知名技术专家，曾就职于百度，当当等互联网公司，对于大数据处理、推荐系统、模式识别等有较为深入的研究。

[19] 交易可锻性（transaction malleability）攻击，又称交易延展性攻击。攻击者侦听比特币P2P网络中的交易，利用交易签名算法的特征修改原交易中的input签名，生成拥有一样input和output的新交易，然后广播到网络中形成双重支付。这样，原来的交易将有一定的概率不能被确认，造成不可预料的后果。

第四章

智能合约[\[20\]](#)

一、智能合约的起源

彼特·托德（Peter Todd）是比特币核心开发者之一。他总结了智能合约（Smart contract）的现状[\[21\]](#)，认为“智能合约讨论的结论是：没有人理解智能合约究竟是什么。如果我们要实施智能合约，应该需要预言机（oracles）”。

确实，要想阐明智能合约的理念和本质并非易事。

我们从智能合约理念的起源开始。“智能合约”概念由计算机科学家、加密大师尼克·萨博（Nick Szabo）于1993年左右提出来。1994年他写成了《智能合约》（Smart contracts）论文，是智能合约的开山之作[\[22\]](#)。

尼克·萨博对智能合约的阐述以一个自动售货机的例子开始。我们可以认为智能合约的原始祖先，是不起眼的自动售货机。在经过潜在的、损失有限的评估后，自动售货机使钱箱里的钱远远少于破坏者付出的代价。售货机根据显示的商品价格收取投币，通过一个简单的机制形成了最初的计算机设计科学，并且有限自动、根据投币金额传递变化和产品。自动售货机是一种搬运合约：任何持有硬币的人都可以与供应商交易。锁定钱箱和其他安全机制保护售货机储藏的硬币和货物不被破坏，从而支撑在各种各样的区域部署自动售货机，并且产生盈利。

在自动售货机概念的基础上，尼克·萨博给出智能合约的定义如下：

“智能合约超越了自动售货机中嵌入各种有价属性的范畴，通过数字方式控制合约。智能合约涉及具有动态性、频繁主动执行属性的财产，且提供更好的观察和验证点，其中主动积极的措施必须丝毫不差。”

尼克·萨博告诉我们的是，智能合约本质上的抽象概念是在个人、机构和财产之间形成关系的一种公认工具，是一套形成关系和达成共识的协定。智能合约的条款（如抵押品、产权划分等）可以嵌入到处理硬件和软件中，以这样的方式使违约成本非常昂贵（甚至令人望而却步）。例如，为房屋而设计出的数字保障智能合约，根据智能合约设计策略，持续完善房屋抵押品协议以便其更充分地嵌入到处理合约条款中。根据合约条款，这些协议将使加密密钥完全控制在具有操作属性的人手中，而此人也将正当地拥有该房屋财产。最简单地，为了防止偷窃，使用者需要完成正确的解锁过程，否则房屋将切换至不可使用状态，比如门禁失效和设施失效等。在传统方式中，如果房屋被用做还贷，有一个令债权人头痛的问题是很难查收赖账的房屋，需要通过频繁沟通才能收回房屋钥匙等。为了解决这一问题，我们可以创建一个智能扣押权协议：如果物主不交费，智能合约调用扣押权协议，把房屋钥匙的控制权交给银行。该协议可能会比雇佣追债人更便宜、更有效。

同时，尼克·萨博提出了智能合约的三要素：

- ①一把可以允许业主同时排除非法第三方的锁；
- ②一个允许债权人秘密接入的后门；
- ③后门只在违约且没有付款的一段时间被打开；最后的电子支付完

成后将永久地关闭后门。

从本质上讲，这些智能合约的工作原理类似于计算机程序的if-then语句。智能合约以这种方式与真实世界的财产进行交互。当一个预先定义的条件被触发时，智能合约就执行相应的合同条款。尼克·萨博关于智能合约的工作理论迟迟没有实现，是因为缺乏天生能够支持可编程合约的数字系统。如果金融机构仍然需要手动批准资产的转移，那么智能合约的目标就没有实现。瑞波实验室的市场和交易主管菲利·拉波波特（Phil Rapoport）说[\[23\]](#)，“实现智能合约的一大障碍是现在计算机程序不能真正地触发支付”。区块链技术的出现和被广泛使用，正在改变阻碍智能合约实现的现状，从而使尼克·萨博的理念有了实现的机会。智能合约技术现在正建立在区块链基础之上，因为区块链本身就是一个计算机程序，智能合约能够与它进行交互，就像它能与其他程序进行交互一样。

在已提出智能合约理念的基础上，结合近几年区块链技术的不断发展，我们将试图给出对智能合约更为具体和详细的阐述。

二、智能合约的定义

智能合约是一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。

承诺定义了智能合约的本质和目的。以一个销售合约为例：卖家承诺发送货物，买家承诺支付合理的货款。数字形式意味着合约需要被写入计算机可执行的代码中，只要参与者达成协议，智能合约建立的权利和义务，就由一台计算机或者计算机网络执行。

我们举个简单的例子，形象化地描述智能合约。

```
If Event_X_Happened:
```

```
Send(爱丽丝, 1000$)
```

```
Else:
```

```
Send(鲍伯, 1000$)
```

意思是：如果事件X发生，则合约给爱丽丝发送1000美元；否则，给鲍伯发送1000美元。

这就是最简单的合约。

如图4-1所示是一个智能合约模型示意，其中各组成部分的定义如下。

①合约参与者：执行智能合约的相关参与者。

②合约资源集合：智能合约执行涉及的参与者资源，比如参与各方账户、拥有的数字财产等。

③自动状态机：智能合约下一步执行的关键，包括当前资源状态判断、下一步合约事务执行选择等。

④合约事务集合：智能合约的下一步动作或行为集合，控制着合约资产并对接收到的外界信息进行回应。

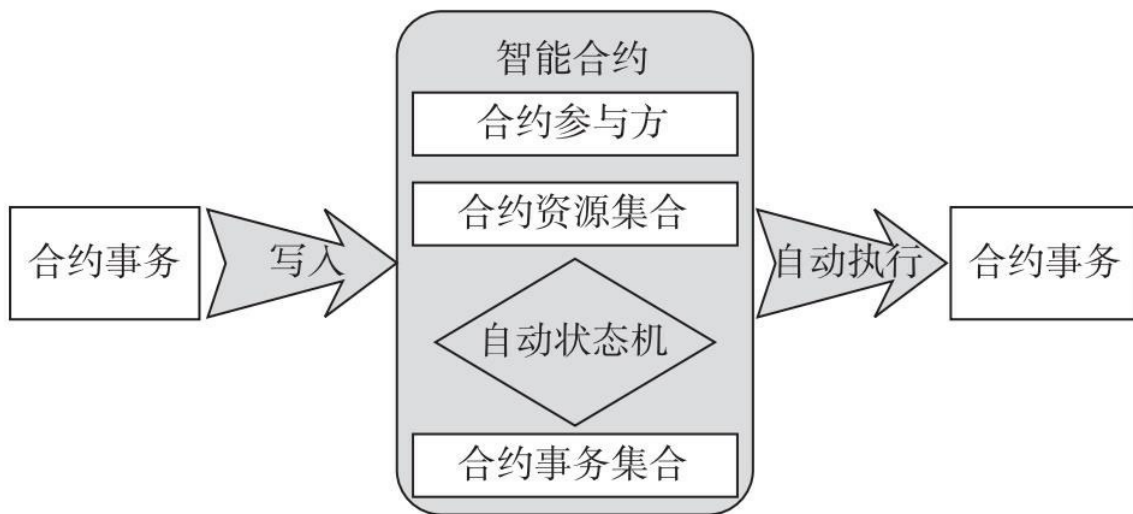


图4-1 智能合约模型示意图

智能合约程序不只是一个可以自动执行的计算机程序，它本身就是一个系统参与者，对接收到的信息进行回应，可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。

智能合约的实现需要底层协议支持，选择哪个协议取决于许多因素，最重要的因素是在合约履行期间被交易资产的本质。再次以销售合约为例。假设参与者同意货款以比特币支付，选择的协议很明显将会是比特币协议。在此协议上，智能合约被实施。因此，合约必须要用到的数字形式就是比特币脚本语言。比特币脚本语言是一种非图灵完备的、命令式的、基于栈的编程语言。

三、智能合约与传统合约的区别

智能合约与传统合约（如法律合约）有相似之处，比如均需要明确合约参与者的权利、义务，违约方均会受到惩罚等。但是智能合约与传统合约存在着显著的区别，表4-1为两者的对比[\[24\]](#)。

表4-1 智能合约与传统合约对比

比较维度	智能合约	传统合约
自动化维度	自动判断触发条件	人工判断触发条件
主客观维度	适合客观性的请求	适合主观性的请求
成本维度	低成本	高成本
执行时间维度	事前预防	事后执行
违约惩罚维度	依赖于抵押资产	依赖于刑罚
适用范围维度	全球性	受限于具体辖区

①自动化维度。智能合约可以自动判断触发条件，从而选择相应的下一步事务；而传统合约需要人工判断触发条件，在条件判断准确性、及时性等方面均不如智能合约。

②主客观维度。智能合约适合客观性请求的场景，传统合约适合主观性请求的场景。智能合约中的约定、抵押及惩罚需提前明确；而主观性判断指标很难纳入合约自动机中进行判断，也就很难指导合约事务的执行。

③成本维度。智能合约的执行成本低于传统合约，合约执行权利、义务条件被写入计算机程序中自动执行，在状态判断、奖惩执行、资产处置等方面均具有低成本优势。

④执行时间维度。智能合约属于事前预定、预防执行模式；而传统合约采用的是事后执行，根据状态决定奖惩的模式。

⑤违约惩罚维度。智能合约依赖于抵押品、保证金、数字财产等具有数字化属性的抵押资产，一旦违约，参与者的资产将遭受损失；而传统合约的违约惩罚主要依赖于刑罚，一旦违约，可以采用法律手段维权。

⑥适用范围维度。智能合约技术可全球采用，适用于全球范围；而传统合约受限于具体辖区，不同国际地区的法律、人文等因素均影响着传统合约的执行过程。

四、智能合约与区块链

（一）智能合约与区块链的关系

尼克·萨博关于智能合约的工作理论迟迟没有实现，一个重要原因是因为缺乏能够支持可编程合约的数字系统和技术。区块链技术的出现解决了该问题，不仅可以支持可编程合约，而且具有去中心化、不可篡改、过程透明可追踪等优点，天然适合于智能合约。因此，也可以说，智能合约是区块链技术的特性之一。

如果说区块链1.0是以比特币为代表，解决了货币和支付手段的去中心化问题，那么区块链2.0就是更宏观地对整个市场去中心化，利用区块链技术转换许多不同的数字资产而不仅仅是比特币，通过转换创建不同资产的价值。区块链技术的去中心化账本功能可以被用来创建、确认、转移各种不同类型的资产及合约。几乎所有类型的金融交易都可以被改造成在区块链上使用，包括股票、私募股权、众筹、债券和其他类型的金融衍生品如期货、期权等。

智能合约看上去就是一段计算机执行程序，满足可准确自动执行即可，那么为什么用传统的技术很难实现，而需要区块链技术等新技术呢？传统技术即使通过软件限制、性能优化等方法，也无法同时实现区块链的特性：一是数据无法删除、修改，只能新增，保证了历史的可追溯，同时作恶的成本将很高，因为其作恶行为将被永远记录；二是去中心化，避免了中心化因素的影响。

基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势，而且可以避免恶意行为对合约正常执行的干扰。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可跟踪、不可篡改。同时，由区块链自带的共识算法构建出一套状态机系统，使智能合约能够高效地运行。

（二）智能合约工作原理

基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，而且事务的保存和状态处理都在区块链上完成。事务主要包含需要发送的数据，而事件则是对这些数据的描述信息。事务及事件信息传入智能合约后，合约资源集中的资源状态会被更新，进而触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据预设信息选择合约动作自动执行。

智能合约系统根据事件描述信息中包含的触发条件，当满足触发条件时，从智能合约自动发出预设的数据资源，以及包括触发条件的事件；整个智能合约系统的核心就在于智能合约以事务和事件的方式经过智能合约模块的处理，输出还是一组事务和事件；智能合约只是一个事务处理模块和状态机构成的系统，它不产生智能合约，也不会修改智能合约；它的存在只是为了让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。

基于区块链的智能合约构建及执行分为如下几步。

- ①多方用户共同参与制定一份智能合约。
- ②合约通过P2P网络扩散并存入区块链。
- ③区块链构建的智能合约自动执行。

步骤①“多方用户共同参与制定一份智能合约”的过程，包括如下步骤：

A.用户必须先注册成为区块链的用户，区块链返给用户一个公钥和私钥；公钥作为用户在区块链上的账户地址，私钥作为操作该账户的唯一钥匙。

B.两个以及两个以上的用户根据需要，共同商定了一份承诺，承诺中包含了双方的权利和义务；这些权利和义务以电子化的形式，编程机器语言；参与者分别用各自私钥进行签名，以确保合约的有效性。

C.签名后的智能合约，将会根据其中的承诺内容，传入区块链网络中。

步骤②“合约通过P2P网络扩散并存入区块链”的过程，包括如下步骤：

A.合约通过P2P的方式在区块链全网中扩散，每个节点都会收到一份；区块链中的验证节点会将收到的合约先保存到内存中，等待新一轮的共识时间，触发对该份合约的共识和处理。

B.共识时间到了，验证节点会把最近一段时间内保存的所有合约，一起打包成一个合约集合（set），并算出这个合约集合的Hash值，最后将这个合约集合的Hash值组装成一个区块结构，扩散到全网；其他验证节点收到这个区块结构后，会把里面包含的合约集合的Hash取出来，与自己保存的合约集合进行比较；同时发送一份自己认可的合约集合给其他的验证节点；通过这种多轮的发送和比较，所有的验证节点最终在规定的时间内对最新的合约集合达成一致。

C.最新达成的合约集合会以区块的形式扩散到全网，如图4-2所示。每个区块包含以下信息：当前区块的Hash值、前一区块的Hash值、

达成共识时的时间戳以及其他描述信息；同时区块链最重要的信息是带有一组已经达成共识的合约集；收到合约集的节点，都会对每条合约进行验证，验证通过的合约才会最终写入区块链中，验证的内容主要是合约参与者的私钥签名是否与账户匹配。

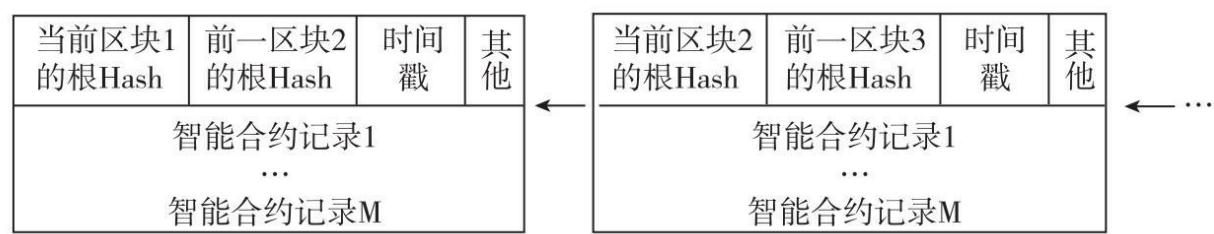


图4-2 合约区块链示意图

步骤③“区块链构建的智能合约自动执行”的过程，包括如下步骤：

A.智能合约会定期检查自动机状态，逐条遍历每个合约内包含的状态机、事务以及触发条件；将条件满足的事务推送到待验证的队列中，等待共识；未满足触发条件的事务将继续存放在区块链上。

B.进入最新轮验证的事务，会扩散到每一个验证节点，与普通区块链交易或事务一样，验证节点首先进行签名验证，确保事务的有效性；验证通过的事务会进入待共识集合，等大多数验证节点达成共识后，事务会被成功执行并通知用户。

C.事务执行成功后，智能合约自带的状态机会判断所属合约的状态，当合约包括的所有事务都顺序执行完后，状态机会将合约的状态标记为完成，并从最新的区块中移除该合约；反之将标记为进行中，继续保存在最新的区块中等待下一轮处理，直到处理完毕；整个事务和状态的处理都由区块链底层内置的智能合约系统自动完成，全程透明、不可篡改。

五、智能合约应用案例

基于区块链的智能合约应用范围很广，应用案例数不胜数，以下仅仅列出一些典型应用。

（一）房屋租赁

假设用户爱丽丝（Alice）与用户鲍伯(Bob)需要构建一个区块链智能合约，目的是爱丽丝将其房屋租赁给鲍伯，租金为1000元一个月，每月支付，租期为一年。假设爱丽丝房屋门锁可通过互联网控制，其开锁密钥为Key（每月生成一次），爱丽丝的银行账户为MA，鲍伯的银行账户为MB。智能合约的执行包括如下步骤：

①爱丽丝与鲍伯提交合约构建申请给智能合约服务器，生成合约并由服务器发布到区块链生效。

②爱丽丝将Key以及MA提供给智能合约服务器。

③鲍伯通过MB向智能合约服务器支付 $1000 \times 12 = 12000$ 元的资金作为抵押，或者鲍伯通过第三方机构的担保，仅向智能合约服务器支付少量资金。

④合约开始执行，智能合约服务器将Key发送到鲍伯，并从鲍伯的抵押资金中扣除1000元，发送到爱丽丝的账户，并生成参与对象记录存入区块链。

⑤每个月智能合约都会定期检查，如果合约未到期，则继续从鲍伯的抵押资金中扣除1000元发送到爱丽丝的账户并发送Key给鲍伯，并生成参与对象记录存入区块链。

⑥整个过程受到第三方机构的监控，所有参与者、第三方机构都可

以通过区块链查询合约执行情况。

⑦租约期限到后，智能合约服务器生成一条合约记录，标示合约终止并发布到区块链，合约执行即终止。

（二）差价合约

金融衍生品是智能合约最普遍也最易于用代码实现的应用之一。实现金融合约的主要挑战是其中大部分需要参照一个外部的权威价值发布者。例如，一个大需求应用是用来对冲密码学货币相对美元或欧元价格波动的智能合约，但该合约需要知道密码学货币相对美元或欧元的价格。最简单的方法是通过由某特定金融机构维护的数据提供合约进行，该合约的设计使该机构能够根据需要更新合约，并提供一个接口使其他合约能够通过发送一个消息给该合约以获取包含价格信息在内的回复，从而支撑智能合约的运行。根据前文描述的智能合约和示例，可以很容易地构建出差价智能合约，在此不再赘述合约内容。

（三）代币系统

基于智能合约的代币系统非常容易实现。其中的关键点是所有的货币或者代币系统，从根本上来说是一个带有如下操作的数据库：从A中减去X单位数据并把它加到B上。其前提条件是：

① A在交易之前至少有X单位数据。

② A批准了进行该交易。

实施一个代币系统就是把这样一个逻辑应用到一个合约中去即可。区块链上的代币系统应用不少，从美元资产到公司股票等。单独的代币具有智能资产、不可伪造的优惠券、与传统价值完全没有联系的积分奖励等多种形式。

（四）储蓄钱包

假设爱丽丝想确保资金安全，但担心资金丢失或者被黑客盗走私钥。于是，她把数字货币放到和鲍伯签订的一个合约里：

①爱丽丝单独一人每天最多可提取3%的资金。

②鲍伯单独一人每天最多可提取3%的资金，但爱丽丝可以用她的私钥创建一个交易取消鲍伯的提现权限。

③爱丽丝和鲍伯一起可以提取任意数额的资金。

正常情况下，每天3%的资金对爱丽丝而言足够了。如果爱丽丝想提现更多， she 可以联系鲍伯寻求帮助。如果爱丽丝的私钥不幸被盗， she 可以找到鲍伯把她的资金转移到一个新合同里。此外，如果爱丽丝弄丢了她的私钥，鲍伯也可以慢慢地把钱提出给爱丽丝。但是如果鲍伯表现出了恶意，爱丽丝可以关掉鲍伯的提现权限，从而保护自己的资金不受损失。

（五）作物保险

很容易且直观的，可以用天气情况作为数据输入创建一个金融衍生品作物保险合约，该合约不是由任何价格指数决定的。如果一个浙江的农民购买了一个基于浙江省的降雨情况进行反向赔付的金融衍生品，那么如果遇到干旱，该农民将自动地收到赔付资金；而如果有足量的降雨，即使没有赔付资金，他也会很开心，因为作物收成会良好。而上述过程利用智能合约可以很方便地实现。

（六）金融借贷

想想看，许多常规的金融交易，律师和银行的工作其实就是重复性

地处理一些简单的任务。但是我们还不得不向律师提供的管理工作或者银行提供的抵押贷款工作支付大量的资金作为报酬。

智能合约能够使这些处理过程自动化和非神秘化，使普通人可以节省时间和金钱，而不用担心被骗。此外，假设你购买房产，可以通过一家银行获得抵押贷款，但通常不会持有长达三十年的贷款。银行只是成为你每月还款的处理者，向投资者支付大头资金，小部分资金用于交税，更小部分资金用于房主的保险。如果贷款还款由智能合约处理，那么贷款处理费用将被取消，省下来的钱可以返还给消费者。最终的结果就是使获得房屋所有权的成本更加低，有利于消费者。

（七）设立遗嘱

虽然智能合约仍然处于初始阶段，但是其潜力显而易见。想象一下分配立遗嘱者的遗产，决定谁得到多少遗产只需简单一列就可实现。如果开发出足够简单的用户交互界面，就能够解决设立遗嘱过程的许多法律难题。一旦智能合约确认触发条件，也就是立遗嘱者已经死亡，智能合约就将开始执行，立遗嘱者的财产将被分割。

（八）证券登记清算

智能合约状态可以包含证券所有权的所有信息。如果登记的证券所有者注意到该合约中证券已经出售给了其他的参与者，其他参与者就会把密码学货币发送到担保账户，然后证券登记信息就会更新，货币就会被转发给原来的证券持有者。无论哪个信息先到达，证券或货币都会保管在一个担保账户中，以避免双重使用。当交易取消或过时后，担保也将取消。以上过程利用智能合约可以轻易实现。

（九）博彩发行

假设对手同意某个在互联网能够访问的数据源，他们就可以对数据

源的价值进行衍生合约或博彩。博彩发行方创建博彩信息，如中奖方式、投注方式、投注时间、奖池钱包地址及密钥，并向该奖池地址充值作为博彩奖池底金；发行方将博彩信息、钱包地址、奖池底金等信息生成博彩智能脚本，写入区块链，被全网用户所知；用户获取博彩信息，开始投注，确定投注目标，并按照博彩规则向博彩钱包地址充值，产生投注记录（含自身钱包地址），写入区块链；产生中奖信息；中奖信息产生后，进行奖金发放以及颁奖记录发布。

六、智能合约面临的问题

智能合约，尤其是基于区块链的智能合约，目前还处在初级阶段，尚未有任何实质性突破和应用，同时也面临着问题与挑战：一是安全性问题；二是私密性问题；三是意外情景问题。同时，人们对智能合约还存在不少的误解。

（一）安全性问题

关键问题之一是安全性及信任度的问题。这与影响区块链实施的问题类似：智能合约系统都被设计成无须信任的环境，这意味着无法改正出现的错误。这是由区块链的不可逆特性决定的。例如，在区块链中，如果你将货币发送给某个地址，这个操作是无法撤销的。因此，如果你与诈骗犯进行交易或者你已经将货币发送到错误的地址中，那么很不幸，金钱损失是无法挽回的。在现实生活中，这些事情可以通过中心化的系统来撤销，但是在智能合约中不行。同样地，在合约代码的设计过程中也有欺诈的问题：某人需要设计（编程）合约，在合约设计时就需要确保没有欺诈的问题发生。对于去中心化的系统，用户只能自己承担相应的风险。

（二）私密性问题

有效利用区块链的一大挑战就是区块链提供彻底的透明度。例如，如果十家银行联合在一起建立一个区块链，其中有两家进行了一项双向交易，这项交易将立即在区块链上对其他八家可见。虽然也可以设计缓解这个问题的各种策略，但目前还没有一种策略可以击败简单有效的中央数据库，除非能有一个可靠的管理员完全控制参与者的权限。

智能合约尤其是基于区块链的智能合约，同样存在这样的问题。每个智能合约都包含了自己的区块链数据库，并且具有完全控制能力。由于区块链数据库中所有的读写操作都是由合约代码主导的，所以其他合约无法直接读取其数据。尽管一个智能合约不能访问其他合约的数据，即一个智能合约无法读取其他合约的数据，但是其数据仍然存储在区块链中的每一个验证节点上。对于每个区块链的参与者来说，完全可以控制一个系统的存储器或者磁盘。如果他们想要从自己的系统中阅读信息，通过计算机手段，是完全可以做到的。

那么，把智能合约隐藏到网页数据中去，就像把它隐藏在代码里一样，是否就可以保证隐私了呢？当然，一般的用户不会看到它，因为它并未显示在他们的浏览器窗口。但是，只需要一个网页浏览器的“查看源文件”功能即可使得隐藏的信息变得普遍可见。同样，对于隐藏在智能合约中的数据，所需要的只是有人修改区块链软件显示合约的代码，就可以看到隐藏的内容。这种修改只要一个水平高的程序员花很短时间就可以办到。因此，智能合约的私密性问题目前还是存在的。

（三）意外情景问题

应当承认，在某一层面上，智能合约听起来确实像一个理想化的场景。如果你不付款，你的汽车将被远程自动收回，这一过程不需要任何人为干预。但是在理论上，智能合约有利的一面是将使金融机构更加乐意接受穷人带来的风险，再也不用担心穷人还不清贷款。如果没有智能合约，穷人可能得不到金融机构的贷款。因为，遇到最坏的情况，如果

借贷人不能偿还贷款，那么收回资产对银行而言，是件轻而易举的事。除了增加获得金融机构贷款的机会外，智能合约也有潜力为没有优势的人打开其他壁垒较高行业的大门。没有智能合约，这些人就没有机会也没有可能获得收益。

尽管在理论上，智能合约听起来非常好，但如何正确、合适地处理意外场景下的合约执行，是一个问题。比如需要收回的汽车正在高速公路行驶的时候，撤销汽车的使用权操作将是十分粗鲁和危险的，而如何准确判断汽车的执行状态也是存在技术难点的。

（四）对智能合约的几种误解

1. 智能合约与协议合同一样

不是这样的。这在前文智能合约与传统合约的区别中已经详细介绍过。根据尼克·萨博对智能合约的定义，智能合约能够让违反协议的一方付出昂贵代价，是通过数字形式掌控现实世界的资产。所以，智能合约能通过执行实现一种特定的需求，能够证明某些条件是否获得满足。这些实现过程都会相当的严格，例如，如果你没能按时完成对一辆汽车的付款，汽车将会被智能合约数字锁定，直到完成支付才会解除。

2. 智能合约具有法律效力

不是这样的。智能合约目前并不能等同于法律，但是它可以代表法律协议的一部分。另外，智能合约合法化工作目前正在进行当中。智能合约的执行结果可以用作审计、追踪，用来证明法定协议的条款是否可以被执行。

3. 智能合约包括人工智能

不是这样的。智能合约本身并不是真的非常智能，也不能等同于人

工智能。智能合约实际上是运行在区块链上的软件代码，由一些外部数据来触发智能合约，外部数据的接收、判断并非人工智能可以实现。此外，对智能合约中其余数据的修改也并非是通过人工智能来实现的。

4.智能合约只能为高水平软件开发者所用

不是这样的。虽然目前的确如此，但是我们很快就会看到与用户更加友好的方法或系统出现，允许商业或个人用户通过图形界面或者简单的文本语言输入来配置智能合约。相信在未来，不需要懂得编程，也能够制定自己的智能合约并顺利执行。

5.智能合约存在应用程序限定

不是这样的。如HTML、C++一样，应用程序受到编写人的控制，智能合约可以成为现实资产、数字资产、智能财产、物联网、通信网和金融工具相互联系的理想方式。智能合约几乎可以应用到所有状态随着时间而改变的事物，并不会受应用程序的限定，参与者类型也多种多样。

七、智能合约的未来展望

智能合约是区块链最重要的特性之一，也是区块链能够被称为颠覆性技术的主要原因，更是各国央行考虑使用区块链技术发行数字货币的重要考量因素，是可编程货币、可编程金融的技术基础。智能合约在今后可能会让人类社会结构产生重大变革，尽管智能合约还有一些需要解决的问题存在。幸运的是，智能合约技术已经从理论走向实践。全球众多专业计算机科学人才、金融界人才也在共同努力完善智能合约。

毋庸置疑，智能合约已经生根发芽了。智能合约是真正的全球经济的基本构件，任何人都可以接入到这一全球经济中，不需要事前审查和

高昂的预付成本。在许多经济交易中，智能合约移除了对第三方的信任，在其他情况下，将信任转移到可以信任的人或机构中。智能合约意味着区块链交易远不止买卖货币这些交易，将会有更广泛的指令代码嵌入到区块链技术中。传统合约是指双方或者多方协议做或不做某事来换取某些物品，每一方都必须信任彼此，并须履行义务。而智能合约无须彼此信任，因为智能合约不仅是由代码进行定义的，也是由代码强制执行的，完全自动且无法干预。智能合约与传统合约本质上都是解决相同问题：以一种方式形成一种合约关系，使得承诺可以执行。只不过它们采用了不同的方法。就这一点而言，智能合约似乎是更好的解决方案，因为智能合约事前执行，不像传统合约一样，事后执行。多重签名智能合约也是未来的一个趋势，比如基于多重签名的交易合约，部分参与者的私钥就可以使用合约中的资金。甚至于，合约可以更加细化。比如参与者共有6人，那么其中的6把私钥里集齐5把就可以花全部资金，如果只有4把则每天最多花20%的资金，只有3把就只能每天花1%的资金等。

在这个蓬勃发展的智能合约领域，尤其是基于区块链的智能合约领域，尽管自动化、高效率和低成本的潜力巨大，但还是有明显的不足。现有区块链技术的一个缺陷就是，智能合约的代码需要向网络内所有参与者尤其是验证者公开。对于很多金融贸易、企业交易来说，这是个巨大的缺陷。因为这就意味着资金投入之后，网络中非参与者可能会了解并积极参与贸易中并给参与者带来麻烦。这同时意味着区块链智能合约的非参与者可以囤积或出售资产，这将损害参与者的利益。此外，尽管智能合约可能给金融服务业带来最具颠覆性的改变，就如同曾经的计算机数据处理带来的变革一样。但是，在实现这个目标之前，我们首先需要清除一些障碍。幸运的是，自区块链技术出现和取得突破之后，智能合约技术已经离开学术的殿堂并走进了社会生活。全球成千上万的互联网金融人才正致力于扩大合约创新的规模，为现代金融机构提供便利。

智能合约的发展可能需要经历漫长的道路，但是更多的智能合约机制正在被设计出来，更多领域的人才正在加入。目前为止，对来自截然

不同的领域，如经济学、密码学、网络科学、金融学的自动化合约执行来说，共同设计研究合约准则是必经之路。如果缺少交叉沟通，无论是对技术的缺乏还是对商业用途模式意识的缺乏，都将造成智能合约的低效。

目前Orisi、Codium、Sympoint、Hedgy、BitHalo、Mirror、Hyperledger、Eris Industries、Ethereum、智能坊、小蚁、Colored Coin、IBM等已经致力于智能合约的平台开发及相关研究，相信智能合约的应用前景一片光明。

参考资料

[1]<http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app>

[2]<https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>

[3] <http://www.wtoutiao.com/p/14dyEMP.html>

[4]<http://www.coindesk.com/smart-contract-myths-blockchain/>

[5]<http://8btc.com/article-1921-1.html>

[6]<http://wangxiaoming.com/blog/2016/03/03/blockchain-2-0-he-yue/>

[7]<http://blockchain.hk/smartcontract/>

[8]Vitalik在中国台湾的演讲：区块链、智能合约和以太坊

[20] 本章由海滨写作完成。

[21] <https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>.

[22] http://szabo.best.vwh.net/smart_contracts_idea.html.

[23] <http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app>.

[24] <http://8btc.com/doc-view-376.html>.

第五章

区块链怎么玩^[25]

^[25] 本章由达鸿飞写作完成。达鸿飞,小蚁创始人,昵称“达叔”,现居上海。中国区块链社区的代表人物,上海浦东国际金融学会金融科技组委员。2013年起全职从事数字货币和区块链技术创新,联合创立了“比特创业营”,多次在北京、中国香港等地的数字货币峰会担任演讲嘉宾。

一、数字货币

(一) 总量恒定型：比特币

尽管区块链的倡导者们有意把区块链技术作为一种中性的独立技术从比特币中抽离出来,但不可否认,比特币是第一个初步成功并引起广泛关注的区块链应用。它在发行机制、分配机制、币值调节机制上有不少创新。中本聪将比特币定义为一种点对点的电子现金系统,“电子现金”一词表明他想要发明的并不仅仅是一个支付系统,而是一套有着独立货币哲学的货币系统。

比特币最常被人提及的特性就是总量恒定。比特币的最高上限为2100万个。在2009年初比特币网络开始运行的最初几分钟内,比特币的数量为零。当大约10分钟过去后,第一个区块产生了,生产出这个区块的矿工也就获得了50个比特币的奖励。这50个比特币就是世界上产生的第一批比特币。通过查询历史数据,我们可以看到最早的这个区块,也就是说区块0的详细信息(见表5-1)。

表5-1 创世区块详细信息

区块#0(主题)	
时间	2009 - 01 - 04 02: 15: 05
难度	0. 999
交易数	1
总转出量	50 BTC
奖励	50 BTC
手续费	0 BTC
矿工	Satoshi
版本	1
区块大小	0. 2099609375 KB
随机数	2083236893
区块 ID	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
币天销毁	0

数据来源：区块元blockmeta.com

可以发现，这个区块产生于2009年1月4日，仅包含了1笔交易，就是那笔“无中生有”新生成出来的50个比特币。在每个区块里，这些新生成的比特币被称作“区块奖励”。由于当时只有中本聪一个人在运行比特币网络，毫无疑问这个区块的产生者就是中本聪本人，这50个比特币的区块奖励也在中本聪的控制下。而迄今为止，这50个比特币都还静静地躺在这个地址里，一次也没有被花费过。

区块奖励并不是一成不变的，每隔4年，区块奖励就会减半。也就是说，2009年开始时，区块奖励是每个块50个比特币，而到2013年，区块奖励就会减半为25个；到2017年，区块链奖励就会再次减半为12.5个；以此类推，直至2100万个比特币分发完毕。这就是比特币的发行机制。图5-1描述了比特币的发行曲线。尽管2030年左右比特币就能达到2000万的发行量，但是要到2140年左右才会达到最终2100万的发行总

量。

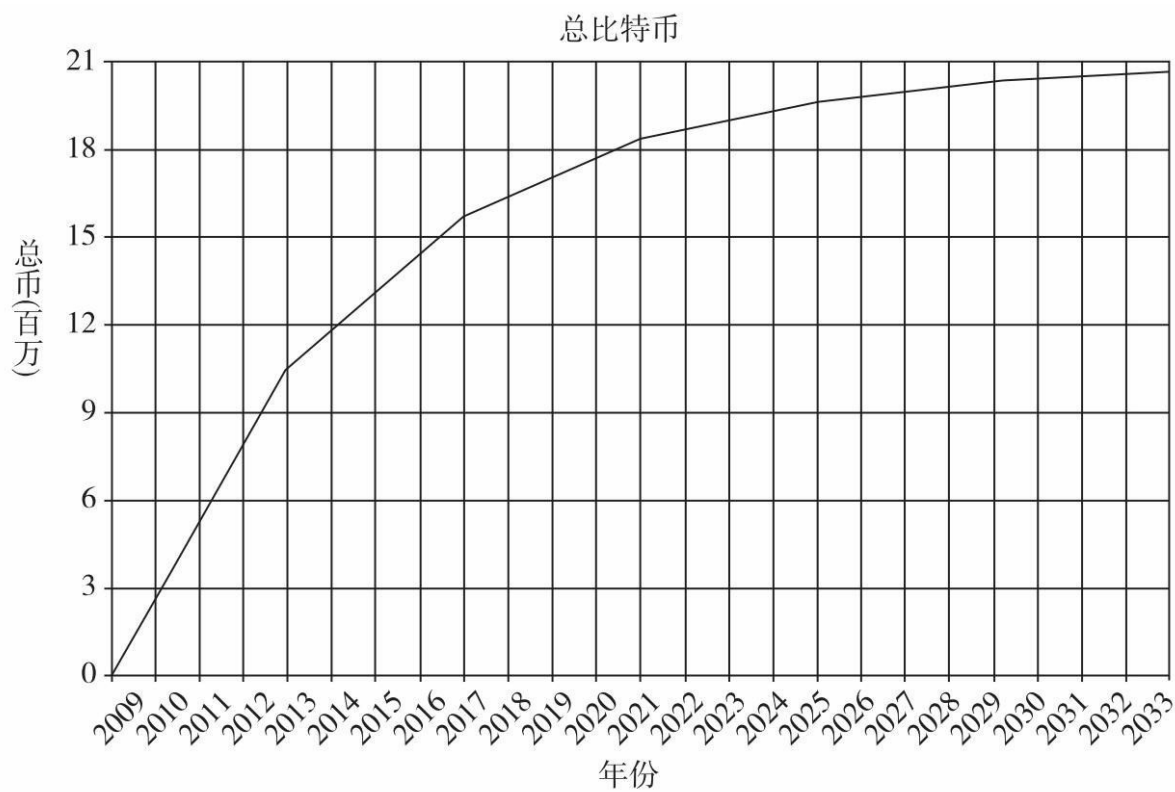


图5-1 比特币发行曲线

比特币通过将新产生的币作为区块奖励分配给矿工（区块生产者）的方式完成整个发行过程。这一过程的最主要特点有三个。

一是发行有严格的既定规则，任何人没有权利修改这些规则，进行规则外的增发。这一约定和经济学家、诺贝尔获得者弗里德曼的观点非常接近。弗里德曼认为，根治通货膨胀的唯一出路是减少政府对经济的干预，控制货币增长。控制货币增长的方法是实行“单一规则”，即中央银行在制定和执行货币政策的时候要“公开宣布并长期采用一个固定不变的货币供应增长率”。

二是发行的主体是不特定的，任何人只要打开运算设备（不管是矿机还是普通计算机）都可以参与到挖矿也就是说货币的发行过程中。这个特点体现了“去中心化”的精神，只要拥有算力，任何人都可参与而不

取决于参与者的身份、地位。

三是存在真实的发行成本，该成本主要包括购买矿机的成本和运行矿机的成本。这些成本的存在“赋予”了比特币某种价值。从经济学角度看，决定价格的并非成本，而应该是市场供需关系。你可以花费数亿美元的成本把一块蛋糕发射到火星之上，但这块蛋糕并不会因此获得数亿美元的身价（如果没有既足够有钱又足够疯狂的疯子的话）。但是不可否认，成本的存在给了市场一个极强的心理预期信号。成本就像是一张比特币市场价格的安全网。回顾比特币的历史价格，每当触及成本时，总会快速迎来反弹。比特币的这种需要成本的发行机制是对布雷顿森林体系瓦解后世界各国无须成本就能发行所谓“信用货币”的一种反讽。

从发行需要成本，发行依照收敛性曲线这些特性来看，比特币模拟的恰好是黄金这种贵金属。和比特币类似，黄金的总量有限，开采需要一定成本。然后，比特币可以跨地域转移、几乎可无限分割、可编程、易保管等特性确实可以完胜黄金这种几千年来人类世界共通的价值存储手段。

然而正因为模拟了黄金的种种属性，比特币也就具备了黄金作为货币时体现出的种种缺点。例如在现阶段，比特币更多地被用作一种投资投机商品，而非货币，导致其价格往往大幅度波动（图5-2），暴涨暴跌阻碍了其成为一种通用的货币。即便我们假设比特币成为一种通用货币，由于总量固定，发行速率既定，比特币无法根据市场的供需而调整货币供应量，也会导致比特币成为一个糟糕的计价单位。当经济发展和财富增长时，以比特币计价的商品的比特币标价反而会持续下跌，物价越来越低。如果这也不是太大的问题的话，更糟糕的是员工的工资可能每半年就要降薪一次，用比特币计价的GDP数据可能是永远停滞不变的，国家可能要提高其他税收来弥补铸币税的消失。人类对价格数字的直觉和数千年积累的经济知识体系恐怕很难适应和跟上这样的变化。

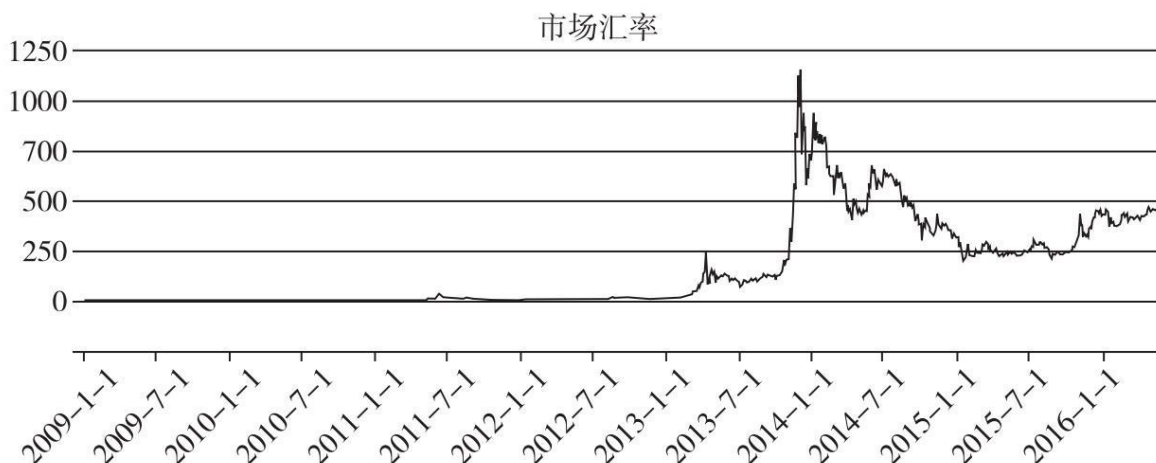


图5-2 比特币市场汇率历史走势图

数据来源：区块元blockmeta.com

（二）锚定型：比特股

非弹性供给的货币会导致币值不稳定，而难以成为一般经济计量单位。如何创造一种能够保持币值相对稳定的货币，一直是数字货币社区的热门话题。这种稳定货币如果被发明，那么基于数字货币的支付结算将会变得非常简单易用。

比特股就是这样一个试图解决这个问题的、基于区块链技术的系统。比特股设计了一套发行“比特资产”的机制。比特资产是一个总称，具体的资产可以是比特美元、比特人民币、比特黄金等。比特股的创始人丹尼尔·拉姆（Daniel Larimer）认为通过其设计的去中心化的发行和交易，各种比特资产将能够锚定各自对应的标的物，实现币值的稳定。比如，比特美元将能够锚定美元的价值，使1比特美元总是等于1美元的购买力。那么具体机制是怎么实现的呢？我们看看比特股维基上的一段描述。

市场锚定指的是比特资产和真实世界中对应的资产在价值上如何保持相等或相近的一种机制。比特股通过提高预测市场的准确度和效率创建一套全新的加密资产，从而锚定如美元、黄金、石油或

者任何其他任何资产。这些资产被称为比特资产（如比特美元、比特黄金、比特石油等）。比特美元是一种在比特区块链上内建交易所交易的数字资产。比特美元跟踪的是真实美元相对于比特股的价值。这种跟踪机制是通过交易行为来确立的，市场上的交易者都预期着比特美元锚定真实美元，这种预期会使他们的交易增强预期的效果。当交易者看到比特股相对美元升值时候，他们会使用更低的以比特股计价的美元的价格来买入美元，因为他们预期着卖出者会用更低的价格抛售。

这种市场锚定基于下面的具体机制。

首先，比特股系统中内置了一种同样名为比特股（简称BTS）的数字货币。BTS的币值和其他数字货币一样是具有高度波动性的。我们可以设计一种机制，用BTS作抵押发行一种新资产，并把这种资产分为A份额和B份额，A份额保持币值的稳定，而由B份额的持有者吸收所有的波动。A份额持有人的收益是获得了稳定的币值，可以用于定价、支付、价值存储；B份额持有人的收益是获得了杠杆，因为其吸收的是A+B整体的价格波动。天底下当然没有免费的午餐。A份额获得稳定币值的交换条件是丧失了BTS币值上涨时的收益权，B份额获得杠杆的交换条件是BTS币值下跌时蒙受的加倍损失。当B份额的市值已经临近临界点，将要不足以覆盖整体波动时，B份额将被平仓。在这里，稳定的A份额就是前文所描述的能够锚定现实资产的“比特资产”。

这样的设计非常类似中国证券市场上的分级基金。但两者的本质区别在于，比特股的设计中，包含A、B份额的类似“分级基金”的发行权是由完全去中心化的市场完成的。任何持有BTS的用户，只要能在市场上找到交易对手方，就能够抵押BTS发行出比特美元、比特人民币、比特黄金这样的比特资产。事实上，用户甚至可以自己和自己成交，发行出A和B份额，然后留下自己想持有的部分，将另一部分通过市场转让出去。在这种设计下，货币的发行权成为一种纯粹的市场行为，因此比

特股创始人丹尼尔·拉姆也就把这样的机制称为“去中心化的央行”。

但是这里还存在一个问题，即A份额相对于什么而言比较稳定。通过同样的抵押机制生成的比特资产为什么有的能锚定美元，有的就能锚定石油？

比特股给出的答案很简单：“仅仅因为名字不同。”当一种比特资产被命名为比特美元时，所有发行、交易的市场参与者都会判断市场中的其他交易者对这种比特美元的价值判断，而其中最合理的假设就是市场中的其他参与者也会认为比特美元的价值应当锚定美元。因此，当比特美元币值高于美元时，会有人抛出获利，当比特美元币值低于美元时，会有人买入等待恢复1：1时获利。这一机制乍听起来似乎纯属臆想，但如果你读过经济学博弈理论就会知道，这是另一个经济学诺贝尔奖获得者托马斯·谢林于1960年在《冲突的策略》中提出的一个后来以其名字命名的著名概念——谢林点。谢林是这样阐述的：

假设明天你要在纽约跟一个陌生人见面，你会选择什么时间和什么地点？这是一个协调博弈问题，其中任何时间、任何地点都平等。谢林询问了一些学生，发现绝大多数的回答是“中午在纽约中央车站”。没有什么因素使“纽约中央车站”成为更好的地点（任何一个酒吧，或者图书馆阅读室都可以用于约定见面），但纽约的文化传统提高了中央车站的保险系数，从而使其成为一个自然的“谢林点”。

在比特资产的例子中，比特美元的谢林点就是美元，比特石油的谢林点就是石油。仅仅是一个名字的不同，在充分市场博弈的情况下，就真的能够各自锚定相对应的实体资产价格！

尽管在理论上，比特股的这套机制是比较合理的。但在实践中，比特资产的锚定还是碰到了不少的问题。首先，比特股的锚定机制相当复

杂，用户首先需要在交易所买到BTS，然后通过比特股的客户端才能发行比特资产。发行过程相当复杂，涉及挂单、平仓、卖空、杠杆等很多复杂的类金融衍生品的概念，普通用户只能敬而远之。

其次，所有比特资产的价值都来自发行时被抵押的BTS的价值。BTS本身的流动性并不太好，因此就容易发生价格波动。而BTS一旦价格波动，就可能会影响到前文所述的高波动的B份额，引发对B份额的平仓，即将B份额所抵押的BTS卖出。这样一来又会造成BTS的价格下跌，引发更多的B份额被平仓。因此，比特股不得不设计了一种熔断机制来进行保护，但熔断也会造成比特资产的价格锚定不准确。

最后，在不同的市场环境下，用户对A、B份额的持有愿望是不同的。市场纷纷预期BTS上涨的过程中，用户倾向于持有B份额；下跌时，则更愿意持有A份额。如果不设计额外的机制来调整A、B份额的动态激励，那么就很容易导致大量比特资产被用户主动平仓，造成比特资产短缺，而不能适应市场需求。

归根结底，由于BTS只是一种虚拟财产，其市场深度和流动性明显不足。以BTS的价值抵押发行比特美元、比特人民币作为一般货币的设计在实践中碰到了较大的问题，难以实现其创始人最初“去中心化央行”的宏大愿景。

（三）政府发行型：央行数字货币

2016年1月20日，来自中国人民银行的一则新闻轰动了笔者的朋友圈，其标题看似非常普通——《中国人民银行数字货币研讨会在北京召开》，然而它的内容却是轰动性的，文中明确指出：

在我国当前经济新常态下，探索央行发行数字货币具有积极的现实意义和深远的历史意义。发行数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少

洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力，更好地支持经济和社会发展，助力普惠金融的全面实现。未来，数字货币发行、流通体系的建立还有助于我国建设全新的金融基础设施，进一步完善我国支付体系，提升支付清算效率，推动经济提质增效升级。

会议要求，人民银行数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，建立更为有效的组织保障机制，进一步明确央行发行数字货币的战略目标，做好关键技术攻关，研究数字货币的多场景应用，争取早日推出央行发行的数字货币。

关于我国央行是否会考虑将区块链技术用于央行数字货币的问题，周小川行长如是说：

“数字货币的技术路线可分为基于账户（account-based）和基于钱包（wallet-based）两种，也可分层并用而设法共存。区块链技术是一项可选的技术，其特点是分布式簿记、不基于账户，而且无法篡改。如果数字货币重点强调保护个人隐私，可选用区块链技术。人民银行部署了重要力量研究探讨区块链应用技术，但是到目前为止区块链占用资源还是太多，不管是计算资源还是存储资源，应对不了现在的交易规模，未来能不能解决，还要看。”

周小川行长所说的基于账户和基于钱包的概念，实质系指基于服务器的电子货币和基于私钥的加密货币。前者即普通电子货币，账户所有权并不真正属于用户，而是托管于服务器之上。后者即以比特币为代表的加密货币，用户拥有账户的绝对专属权，不仅可以用自己的密钥开启，还可以通过智能合约授权别人拿密钥开启，账户的控制权归根结底在用户端，商业银行也未必有权开启。

英国央行也正在全面探索区块链技术，数字货币被纳入了英国央行在未来一年的研究重点。英国央行货币政策二把手本·布劳德本特（Ben Broadbent）曾在一次讲话中指出：比特币可能无法得到广泛应用，但由央行发行的数字货币可能对全球金融体系产生巨大影响。“去中心化的虚拟票据交易所和资产登记处”可能会是这项技术更好的探索之路。

澳大利亚央行也是探索数字货币和区块链技术的先行者。澳大利亚储备银行（Reserve Bank of Australia）支付政策部门主管托尼·理查德（Tony Richards）就建议，在将来某个时间澳元应该转换成数字货币形式。他特别指出：“可行的方案是由中央银行发行货币，再由授权机构监管货币交易和流通，当然现有的金融机构可能会参与其中。”

各国央行发行数字货币的出发点很简单。首先，纸钞的流通成本太高。据美国零售商和银行估计，持有实物美元的年均成本在60亿美元左右，其中包括会计、储存、运输和安全成本。纸钞逐渐退出交易已经是大势所趋。一旦纸钞退出交易，那么央行就和货币的使用者切断了所有的直接联系，用户使用的不再是央行直接发行的货币，而是银行、第三方支付所发行的IOU（欠条），央行的货币政策将更难被传导至市场。其次，日本和北欧国家央行已经在实施所谓的负利率，然而负利率只能传导到金融机构而无法传导至个人。因为一旦在个人层面实施负利率，那么个人的第一反应就是从银行提取现钞，那就会造成全国范围的挤兑和银行业危机。相反，如果现钞退出市场交易，央行就可以更好地实施包括负利率在内的货币政策，从而更强地影响市场。这也是荷兰央行用DNBCoin、英国银行用RSCoin进行数字法币概念验证的出发点。

二、支付汇兑

关于货币的定义，学过政治经济学的朋友恐怕对这句话都耳熟能详，“货币具有价值尺度、流通手段、贮藏手段、支付手段和世界货币

五种基本职能”。实际上后两者是前面三种手段的派生。现代经济学著作中，一般认为货币的本质只有三个，即交换媒介（medium of exchange）、价值存储（store of value）和计价单位（unit of account）。然而比特币的出现挑战了这一货币定义。即便在比特币白皮书发表七年后的今天，比特币的波动仍然较大，至少和有一定波动率的单只股票相当。而价值存储和计价单位这两个货币职能都要求货币的币值相对稳定。但是，比特币却切切实实可以被用作交换媒介来完成支付，特别是跨境的支付。

假如你想购买一个美国互联网公司的云计算服务，需要支付100美元，而你既没有信用卡也不愿去银行办理国际电汇，要怎么办呢？你可以：

①在中国的比特币交易所花大约650元人民币买入价值100美元的比特币；

②将这些比特币立即提出，并转入美国的比特币交易所；

③将这些比特币卖出并获得100美元，将这100美元提现至上述云计算公司的收款账户。

由于比特币本身良好的全球流动性，在这里很好地起到了交换媒介的作用。由于在整个流程中，用户持有比特币的时间一般不超过1小时，也就无需承受太大的波动风险。这里的比特币已经部分起到了货币的作用，但又仅仅作为交换媒介，而非价值存储和计价单位。

在支付汇兑这一领域，目前领先的有BitPay、Circle、Coinbase这三家公司。它们都想通过比特币网络建立起一个类似VISA/万事达的全球支付网络。BitPay选择了面向商家，直接提供支付处理服务，而Circle、Coinbase选择了面向消费者提供钱包和买卖服务。

BitPay进入最早，成立于2011年。2014年5月，BitPay获得了当时数字货币领域最大的一笔投资——3000万美元的A轮融资，公司整体估值也达到了1.6亿美元。BitPay的早期投资人中还包括了香港亿万富翁李嘉诚的Horizons Ventures（维港投资）。时至今日，BitPay的客户已经包括微软、PayPal等知名公司。

BitPay为商家提供接受比特币付款的服务，并实时生成以比特币计价的价格。回到上面的100美元的收款例子，如果这家公司接入了BitPay，那么用户会发现多出一个用比特币支付的选项，并且此时的比特币计价的价格会每15分钟按照比特币的市价发生变化。用户可以直接用已有的比特币支付，没有的话就自行在交易所购买。对商家来说，可以直接把收到的比特币保存，也可以要求BitPay及时按照市价帮他卖出，而直接获得100美元。

那么为什么BitPay不提供完整的三步服务？原因在于监管。美国有严格的金融监管制度，BitPay在现有的服务模式下，其需要的金融牌照较少。如果提供完整的三步服务，那么就要面临严格的反洗钱、KYC（了解你的客户），甚至是KYCC（了解你的客户的客户）等监管挑战。由于美国是联邦制国家，在美国50个州申请一遍金融牌照可不是“好玩”的。不是财大气粗的公司，根本玩不起这个游戏。最近一轮融资额达到3000万美元的BitPay也还没有能力收集齐所需的牌照。

然而世界“土豪”总是有的。2015年，Circle获得了高盛、IDG（美国国际数据集团）等机构的5000万美元投资。Circle的商业战略就是跑马圈地拿各种牌照，处理和政府关系是它的强项。2015年9月，Circle第一个获得了美国纽约州的BitLicense。2016年4月，Circle又第一个获得了英国政府颁发的电子货币牌照。正因为各种牌照在手，Circle提供了买入、卖出、支付等全套比特币支付服务。而且用户在Circle的美元余额还能受到美国联邦存款保险制度的保障。不过，牌照是把“双刃剑”，严格的监管压力也导致Circle的用户体验下降。

说到支付汇兑不得不提的另一个项目叫作Ripple。Ripple是一个甚至比比特币还古老的项目。我们今天熟知的Ripple则是2012年由杰德·麦克莱伯（Jed McCaleb）和格瑞恩·拉森（Chris Larsen）接手后的Ripple Labs公司主导的Ripple。

Ripple的理念是SWIFT 2.0。SWIFT（Society for Worldwide Interbank Financial Telecommunication，即环球同业银行金融电讯协会）是一个国际协作组织，运营着一个全球性的金融电报网络。银行和其他金融机构通过它与同业机构交换电报，从而完成金融交易。

当用户甲通过中国的A银行向美国B银行的用户乙汇款100美元时，有如下两种情况。

1.A银行和B银行有直接合作关系

A银行首先向用户甲收取100美元和对应汇费，然后通过SWIFT网络发送一份电报给B银行，通知B银行向用户乙的账户存入100美元。尽管这100美元并没有真的从中国移到美国，但用户乙已经收到款了。由于A、B银行有合作关系，它们彼此有一定的信任额度，可以过一段时间清算一次彼此的欠账关系，做一次结算。

2.A银行和B银行没有直接合作关系

这时就比较复杂了。A银行不能直接给B银行发电报，因为B银行并不认可A银行的指令。此时A银行就只能寻找一间和A银行、B银行都有合作关系的C银行。A银行向C银行发电报，C银行再向B银行发电报。如果找不到这么一间C银行，还可能需要经历A银行→D银行→E银行→B银行的路径。

以上的流程看起来似乎很快就能完成，但是由于SWIFT成立于1973年，是诞生于电报技术年代的产物，大量的流程设计需要人工参与。一

笔SWIFT汇款，短的话也要几天时间，长的话甚至可能超过1周。同时，SWIFT网络的运行成本高昂，导致了国际汇款费用较高。以中国银行为例，每笔SWIFT汇款需要150元的电报费加上汇款金额千分之一的汇费。更糟糕的是每个中间行、收款行都会进行几美元到几十美元的扣款操作。尽管你在100美元之外，已经额外支付过了电报费、汇费，对方实际到账的却也往往只有90美元甚至更少。扣费的多少取决于中间经过多少和哪些中间行，扣费金额在用户汇款前是无法准确获知的。低速、昂贵的SWIFT系统成了国际汇款，特别是小额汇款的障碍。

Ripple便是为了解决这个问题而诞生。在Ripple协议中，各个银行可以把用户的银行余额搬到Ripple系统中来。一些做市商会在Ripple内置的交易市场里进行类似于“A银行人民币：B银行美元”这样的挂单。比如当前美元兑人民币的汇率中间价是6.5：1，那么做市商就会挂出6.51：1，卖出银行B美元同时买入银行A人民币，挂出6.49：1，买入银行B美元同时卖出银行A人民币的挂单。当银行A的用户甲想要向银行B的用户乙汇款时，神奇的事情发生了：用户甲只需要表示准备向用户乙转账100美元，此时Ripple系统会在各个内置市场里自动寻找最优的汇款路径，并自动完成兑换、汇款的全过程。一般情况下，用户甲在银行A的人民币会被直接兑换成在银行B的美元，而某些时候可能绕个圈子更便宜。比如系统会帮你发现把银行A的人民币先兑换成银行C的日元再兑换成银行B的美元更划算。

Ripple就像一个货币的同声传译，无论对方需要什么货币，你只需要提供你在Ripple里的有价值的资产，系统就能自动帮你找到最优的兑换路径，并完成汇兑的全过程。在Ripple系统里，比特币这样的交换媒介不再是必需品。银行一旦接入Ripple系统，其用户的存款余额就可以被数字化，从而拥有和比特币类似的流动性，在Ripple网络里自由流动、自由兑换。

Ripple的发展也不是一帆风顺的。其架构设计注定了其在合规性、

隐私性和可扩展性上的短板，银行也对直接使用Ripple公司的服务并不感兴趣，而更愿意自建系统，自组联盟。对此最直接的印证就是包括高盛、JP摩根、巴克莱、瑞银等40多家银行加入了2014年才成立的R3联盟，而Ripple阵营的银行却屈指可数且并不知名。Ripple的商业前景还未明朗。

三、登记结算

银行间的支付汇兑只需要记录一种资产类型，即货币。而当一个系统除了货币还可以被用于其他各种类型资产的权益归属、份额转移和流转交易时，这个系统就具备了登记结算的能力。区块链的分布式账本技术备受关注，而分布式账本最适合的应用场景就是登记结算业务。

在中心化账本体系下，为了追求数据的一致性和单一真相来源（single source of truth），A、B、C、D这些市场参与者把记账的任务托付给了中央登记结算机构，并约定大家一致认可登记结算机构处的账目为最高效力的账本。因此，这些中央登记结算机构需要非常强的公信力才能被各个市场参与者所认可，而建立和维护这样的公信力需要极为繁杂的内部规章和外部审计流程。

在分布式账本体系下，每一个市场参与者都维护一份全市场的账本，各个参与者通过区块链技术对各自的账本进行实时同步，保证账本内容的一致性。这使得分布式账本做到了在物理上的多点分布和逻辑上的数据统一。参与者当然有能力篡改自己的账本，但是区块链技术的底层密码学实现保证了这只能骗骗自己，而无法欺骗其他市场参与者。

在计算机科学中，想要在分布式系统下取得数据一致性有两种思路，分别被称为共享存储（Shared memory）和消息传递（message passing）。区块链技术兼具两种思路，通过点对点网络的共享存储和不

停的消息传递，实时同步各自的账本从而实现数据一致性。

区块链技术怎样应用于登记结算业务？让我们先从登记和存管说起。在证券市场形成的早期，股票都是实体的纸质凭证。进行交易时双方就需要一手交钱，一手交票，非常烦琐。尤其当货币可以记账式支付后，股票的纸质凭证的实体转移成为制约股票交易速度的瓶颈。于是存管业务出现了，即投资者把股票的纸质凭证存放在各自的券商处，当发生股票交易时，只需要券商和券商之间在股票上做背书过户的工作就可以了，投资者不再直接持有股票。

随着上市发行的股票越来越多，股票交易越来越频繁，这种以人工操作为主的实物股票背书过户制度越来越阻碍了证券交易的发展。1968年美国出现了纸上作业危机。为了解决这一危机，美国设立了中央证券存管机构（CSD，central securities depository），即美国证券存管信托公司（DTC）。

中央证券存管机构出现后，证券交易出现了非移动交收（immobilization）和无纸化（dematerialization）的重大升级。首先是纸质凭证都被中央证券存管机构集中管理，发生流转交易时，不再需要做任何物理上的移动工作，而仅仅是在一个账本上更新这份股票的拥有者，实现了非移动交收；然后，市场逐渐发现纸质凭证已经没有任何存在的实质意义了，只要有一份大家公认的账本，就能够完整地记录股票的归属，于是股票不再是上市公司自身发行登记的纸质凭证，而成为上市公司在中央证券存管机构电子化登记账目，实现了证券的无纸化。

对于登记和存管，可以说区块链的分布式账本是极佳的解决方案。区块链上的任何资产天然就是以无纸化和非移动形式交收的。用区块链实现的电子化登记账目可以在没有中央证券存管机构存在的情况下，由各个市场参与者分布式的分会维护更新，实现CSD所能提供的完整功能。而且区块链的智能合约还能实现证券的代码化，让证券变成可编码的智能资产。股票的分红派息、股东投票、禁售限制等可以程序化实

现，将人工操作降到极低。

说完登记和存管，就要说一下结算了。结算是清算和交收的统称。清算类似于轧差，通俗地说就是如果我昨天吃饭借了你10元钱，你昨天买水又借了我3元钱，那么轧差后我就只需要还你7元钱了。可以想象如果有100个人，彼此间都相互借过钱，那么这时候需要轧差的交易对可就乱如一团麻了，而且一旦有人违约，还可能造成难以预计的风险传递。因此，在现代证券交易里，中央对手方（CCP，central counterparty）模式成为一个常用的轧差方式。有中央对手方存在的轧差就叫作清算。在中央对手方模式下，A和B之间的交易被拆分成了A和CCP，CCP和B的两笔交易。对于A、B来说，就不再需要担心对方的支付能力，CCP会保障交易的完成。

清算就是算账，账算完后，就是交收了。只有清算、交收都完成了，才是结算完成，交易成功。交收时，结算机构把A卖出的证券登记给B，“同时”把B的货币划拨给A。

上面的模式看起来很完美，但是却存在着问题。首先，中央对手方模式是一种“大而不倒”式的安全。把分散纠缠的风险都堆放在一起，并不等于风险就不再存在了。中央对手方的优点是隔离了风险传递，但代价是把风险都聚集到了中央对手方一个人的身上。最终的走向有可能会像2008年次贷危机中的银行一样，一旦发生危险，国家就不得不动用国家财政来拯救。其次，细心的读者可能发现上一段最后一句话里的“同时”是打了引号的。是的，这里的同时只是一种希望。由于资金的划拨是通过银行体系，证券的转让是通过中央登记存管机构实现的，是没有办法做到真正的原子级的货银对付的，交钱和交货总有先后。

那么能否找到解决这些问题的终极方案呢？区块链也许是一个答案。

通过区块链的分布式账本技术，理论上可以完全消灭轧差/清算的

过程。正是由于现存证券交易系统技术和流程上的低效，资金和证券登记的割裂，才导致了清算、交收环节存在的必要性。

在区块链技术下，首先资金和证券可以在同一个账本中登记，从而保证原子操作级的货银对付。所谓原子操作，即指交钱和交货这两个动作被包含在一个不可分割的操作指令中执行，要么同时成功，要么同时失败。任何意外，无论是突然断电还是断网，都不可能导致钱付了而证券没有转移成功。

其次，中央对手方存在的必要性来自于多边轧差的混乱和可能产生的风险传递，而代价就是把风险集中到了中心点上，这意味着中央对手方就是一个单点故障源（Single Point Of Failure）。而区块链技术可以实现证券交易的实时全额结算（RTGS, Real-time gross settlement）模式，完全避免了轧差/清算的业务流程，让交易和结算成为一个动作，不再存在结算（清算、交收）这一过程。没有了清算、交收流程，中央对手方也就不再有存在的必要了。由于一次交易一笔结算，原来错综复杂的多边轧差关系也不复存在，世界一片清净。

当然，尽管理论上区块链可以完全消灭清算、交收流程，但由于网络宽带、存储容量、延迟性要求等技术条件的限制，在要求高频、高吞吐、低延迟的证券交易领域，基于区块链技术的实时全额结算的登记结算系统还难以胜任。基于区块链技术的登记结算目前更适合用于低频、低延迟要求的场外交易系统。

在纳斯达克上市的电商公司Overstock就以此为理念，利用区块链技术开发出了一个名为T0的证券交易平台。顾名思义，T0意味着T+0结算，是对美国现存T+3股票结算的巨大超越。T0近期收购了一间ATS（另类交易系统，有点像中国的互联网证券）公司，并已经得到了美国证券监管机构SEC的许可，将在2016年下半年发行Overstock的股票。未来，投资者既可以在既有的纳斯达克市场内，也可以通过合规的ATS交易系统在T0平台上购买到Overstock公司的股票。如果T0上的价

格、流动性都不错的话，也许越来越多的公司会愿意到T0上发行股票。T0的口号是对基于区块链技术的证券登记结算系统的一个很好的诠释：The Trade Is The Settlement(交易即结算)。

纳斯达克当然也不甘示弱，通过和区块链技术公司chain.com的合作，推出了自己的非上市公私股权登记系统LINQ。有意思的是，2015年12月LINQ上第一个登记股权的公司也是其合作开发方chain.com。目前有6家和区块链技术相关的公司成为LINQ的首批内测客户。纳斯达克使用区块链技术布局非上市公司的意图有两个：一是全球资本市场越来越青睐于一级市场，大量独角兽公司迟迟不上市，越来越需要一个一级市场的登记流转服务，因此纳斯达克还收购了专注于上市前公司股权转让服务的SecondMarket（二级市场）；二是作为一个金融服务公司，纳斯达克有大量的技术输出服务，为全球几十个资本市场提供技术服务，区块链方向的技术储备会为未来几十年的技术输出业务提供基础。

同时，各国的证券交易和登记机构也没闲着。澳大利亚证券交易所ASX和美国的中央证券登记结算机构DTCC，先后宣布与区块链技术初创公司DAH（Digital Asset Holdings）合作，开发基于区块链技术的登记结算系统。东京证券交易所JPX也在和IBM以及野村综合研究所进行区块链登记结算的概念验证工作。伦敦证券交易所LSE则牵头成立了“交易后分布式账本工作小组”（Post-Trade Distributed Ledger Working Group）这一技术联盟。此外，纽交所NYSE、多伦多证券交易所TSX、芝加哥商品交易所CME、韩国证券交易所KRX等也都在区块链领域进行探索。

国内也有一个类似的项目：小蚁（AntShares）。小蚁是一个用来登记结算各种数字资产的区块链底层协议，而其中一类数字资产就是公司股权。公司可以将自己的股东名册放到小蚁区块链上进行管理，公司的投资者们用电子签名在区块链签订股权转让的电子合同，由区块链保证货银对付，实现公司股权的数字化流转。有两类公司在现阶段就非常适

合使用小蚁。

第一类是进行股权众筹的公司。这些公司在股权众筹完成后面临管理大量股东的问题。股权的变更登记费时费钱费力。利用小蚁区块链，众筹投资者不仅可以在线上完成股权登记的所有电子合同，还能非常方便地进行股权的再次转让，为股权众筹提供了良好的退出机制。

第二类是进行员工持股激励方案的公司。这些公司原本的员工持股激励方案往往都是落在一份份的纸质文件上，而没有一个完整的数字化的股权激励管理系统。使用小蚁后，公司可以把股权、期权、限制性股权、虚拟股权（分红权）等各种权益在一个去中心化的区块链系统里管理起来，而员工则能够自己掌控自己的权益份额，感受到实实在在的激励。利用小蚁，公司还可以将投票权和经济权益分离，实现更好的管理架构。

在全球区块链行业会议Consensus 2016上，美国特拉华州州长宣布了一个令人震惊的消息：特拉华州将修改其公司法，允许公司用区块链技术登记股权，实现公司注册的流程简化，并更好地对股权归属进行追踪，更好地实现股权的流转交易。在特拉华州注册的美国公司超过100万家，其中包括美国一半以上的上市公司和超过65%的财富500强公司。特拉华州的举动将深刻地影响美国国家层面的公司股权登记体系。

现有证券市场的登记结算制度是历史演变的产物，其业务流程较长，参与主体复杂，导致了清算、交收的效率低下，往往要T+1甚至T+3才能真正完成交易。冗长的结算流程导致了更久的资金占用和更长的风险敞口。基于区块链技术的登记结算系统，有望实现低摩擦的登记存管流程，从中央证券存管模式转换到分布式账本存管模式；有望消灭部分低频应用场景下的清算、交收过程，从而使这类场景不再需要中央对手方这一角色，代之以实时全额结算模式。

四、数据存证

前面花了较大的篇幅介绍了区块链技术在数字货币、支付汇兑、登记结算这三大领域得以应用的内在逻辑。理解了这些内在逻辑后，就会发现，区块链在其他领域的应用往往“万变不离其宗”，总是这三种应用场景的某种变形。那么我们就先来看基于区块链的数据存证应用。

基于区块链的数据库有一个核心的特点是不可篡改。前面说过，你可以篡改你自己手里的那份账本，但那只能骗骗你自己，骗不到别人。你可以在自己的脸上写上“我是刘德华”，但全社会每个人头脑里的账本上都记录着刘德华的长相，你只能照镜子骗自己，骗不到其他人。基于不可篡改这一特点，区块链就是一个非常好的数据存证技术。

成立于2012年的存在性证明（Proof of existence）项目可能是这个领域最早的实践者。在其官网上，用户可以把一个本地的文件拖入浏览器。这个文件本身不会被上传，而是会在本地浏览器内进行一次摘要计算，计算出此文件的数据指纹——哈希值。这个哈希值会在10分钟左右被“存在性证明”网站通过一笔交易写入比特币的区块链。从而这份文件的数据指纹就永久性地被公开保存在了比特币区块链上。

值得再重复一遍的是，公开保存在比特币区块链上的仅仅是该文件的简短的数据指纹。通过数据指纹是无法反推出任何有关该文件的信息的，哪怕是文件大小也不行。文件一直留在用户本地电脑上，不会被公开或上传给“存在性证明”官网。

用户可以将“存在性证明”这样的服务用于三个目的。

①知识产权保护。用户可以把自身创作的作品、专利的数据指纹通过“存在性证明”网站记录到比特币区块链上。当未来发生版权纠纷时，用户通过展示区块链上的数据指纹，证明自己早在某某时间就已经拥有该份文件。如果对方无法提供更早的证明，再结合其他证据，就很容易

推定你是该知识产权的创作者。

②给文件盖时间戳。你可以把一份合同、一份文档的数据指纹通过“存在性证明”网站记录到比特币区块链上，从而为这份合同、文档盖上一个时间戳。通过区块链向外界证明在某个时间点，这份合同、文档就已经存在了。

③完整性校验。当你把一个文件的数据指纹通过“存在性证明”网站记录到比特币区块链上后，未来你就可以校验这份文件是否被篡改过。比如微软可以把Windows的安装镜像的数据指纹上传至比特币区块链，任何用户从第三方网站下载到Windows安装镜像后，都可以通过比特币区块链比对数据指纹是否一致，从而发现该安装镜像是否遭到了恶意软件的篡改。

这个领域另一个著名的区块链项目叫作公证通（Factom）。Factom这个名字取自拉丁语Factum，意为“确定的事实”。和“存在性证明”相比，公证通的架构更为完整。公证通是这么介绍自己的：

公证通旨在借助区块链技术，为大型的私营或公有机构安全地存储数据。公证通将这些数据进行编码或者生成数据的独一无二的特征码（哈希），然后将其存储在公证通系统内不可篡改的分布式账簿中。账簿中的这份不可篡改的数据可以被用来作为某份数据的“存在性证明”，也可以为未来的商业活动提供“事实来源”。

公证通也可以被理解为一个不可撤销的发布系统，（公证通系统中的）数据一经发布，便不可撤销。公证通的这个特性提供了一份准确的、可验证的且无法篡改的审计跟踪记录，消除了（人类活动中的）盲目信任。

与“存在性证明”网站上传数据指纹不同，公证通还提供了一套分布式存储原始数据的存储网络。数据指纹被存储于比特币区块链，数据原

文被存储在公证通自建的分布式存储网络。存储在公证通存储网络的数据将每隔十分钟被计算一次数据指纹，并将数据指纹上传到比特币区块链，从而使得公证通本身也无法修改用户的原始数据。

尽管公证通能够存储数据原文，但由于其经济模型的设计，每GB的存储成本超过1000美元。公证通并不适合当网盘来使用存储一般性数据，而更适合保存精简的需要审计的关键性数据。

与Factom、Proof of existence类似的项目还有Stampery、Bitproof等。

五、知识产权保护

把区块链技术与知识产权相结合是目前比较热门的区块链应用场景之一。一是有极高的市场需求，从每年的“3·15”维权热度可以看出，知识产权的维权存在取证难、周期长、成本高、赔偿低等一系列问题；二是区块链具有的功能恰好匹配了这种市场需求，维权难的关键原因是第三方执行效率低下，而区块链通过程序算法自动记录信息，移除了第三方，信息储存在互联互通、共享的全球网络系统中，无法被任意篡改，极大地提高了维权的效率。

知识产权保护的第一步是确认知识产权是何时生成的。具体到版权这类知识产权来说，一直以来存在两种不同的实践：一种规定必须经过登记程序的作品才享有完整的版权；另一种则规定只要作品创作问世版权就生成了。美国过去一直实行第一种实践，即经过登记的作品才享有版权，而近年来通过修改版权法，美国开始和世界其他大部分国家一样接受了创作问世即版权生成的做法。

尽管如此，当碰到侵权、诉讼、版权转让等情形时，未经登记的版权仍然面临种种不便。而在美国版权办公室每登记一件作品就要35~55

美元的支出。考虑到今天大量在互联网上发表的海量文字、图片、视频，为每件这样的作品注册版权几乎是不可能的任务。基于区块链的版权登记能够很好地解决上述问题。

①区块链的开放性让任何人都可以在全球任何角落向区块链写入信息。不管是在凌晨3点的西雅图不眠之夜，还是在横跨大西洋的量子号邮轮，只要能连上互联网，版权登记就不受时间、空间的限制。

②区块链上的信息一经写入就无法篡改。无论是上传者本人，还是相关机构都无法对历史进行修改。信息一旦写入，时间戳就把这段信息永久地封存，无法篡改。

③区块链的登记将能做到几乎免费，让更多的作品有可能被登记。

④在区块链上可以很方便地实现链上版权交易。

Mediachain在区块链与分布式文件系统（IPFS）基础上推出元数据协议，允许数字创意者在他们的创作作品上附加信息，并在数据上添加时间戳传送到比特币区块链，然后存贮在IPFS。后者是一个整合了区块链技术的点对点文件系统。

Monegraph则侧重区块链的版权交易，其产品的用户体验和其他图片分享销售网站无异：创作者上传自己的作品形成作品集，Monegraph的手机App将其展现给潜在的买家，并形成交易。但在技术上，Monegraph使用区块链对每件作品进行确权登记，并在发生授权使用和权利转移时进行相应记录。

此外，从事知识产权方向的区块链项目还有Verisart、Blockai等。

六、溯源、防伪与供应链

溯源，顾名思义就是追踪记录有形商品或无形信息的流转链条。通过对每一次流转的登记，实现追溯产地、防伪鉴证、根据溯源信息优化供应链、提供供应链金融服务等目标。把区块链技术应用在溯源、防伪、优化供应链上的内在逻辑和前文所述的数据存证场景非常类似——数据不可篡改和加盖时间戳。

传统的溯源系统要么使用今天的中心化账本模式，要么由各个市场参与者分散孤立地记录和保存，是一种信息孤岛模式。

在中心化账本模式下，谁作为中心维护这个账本变成了问题的关键。无论是源头企业保存，还是渠道商保存，由于其自身都是流转链条上的利益相关方，当账本信息不利于其自身时，其很可能选择篡改账本或者谎称账本信息由于技术原因而灭失了。这样的例子在现实生活中屡见不鲜，摄像头总是在关键的时候没被打开，又或者刚好损坏。因此，利益相关方维护的中心化账本在溯源场景下是不可靠的。

信息孤岛模式下，市场的各个参与者自我维护一份账本，这样的账本俗称台账，电子化后又被冠上进销存系统的名字。不论是实体台账还是电子化的进销存系统，拥有者都可以随心所欲地进行篡改或集中事后编造。例如我国工商部门强制要求的食品台账制度，在落到小企业、个体经营者层面时，往往变成了一种为了应付检查而突击编造的形式主义。而且这些上下游链条的台账之间没有互通互联，各自是一个独立的信息孤岛，无法做到快速的追溯问责。

区块链在登记结算场景上的实时对账能力，在数据存证场景上的不可篡改和时间戳能力，为溯源、防伪、供应链场景提供了有力的工具。

位于英国伦敦的区块链初创公司运营了溯源领域的一个知名项目——Everledger。Everledger是一个用于登记钻石身份和记录钻石流转过程的区块链。Everledger的主要客户是承接钻石偷盗险的保险公司。保险欺诈是欧美保险公司最头疼的问题。美国和欧洲的保险公司因为保险

欺诈每年要损失450亿英镑，经管保险公司的年度反欺诈支出高达2亿英镑，65%保险欺诈无法破案。这其中，每年约有1亿的金額被用于珠宝的失窃赔付。

Everledger正是瞄准了这样一个市场。通过和美国、安特卫普、以色列、印度等地的钻石鉴定机构合作，Everledger利用钻石的4C信息（颜色、切工、纯净度、克拉）外加14个特征数据，为每个钻石生成一个独立编号。通过在区块链上记录这一编号的流转过程，Everledger可以转载钻石的归属和所在地。当钻石不幸失窃时，保险公司在Everledger上将该钻石标记为被盗。这个钻石无法再次投保，如果被用于抵押也很容易被接受抵押的机构在Everledger上查找到，同时还为执法机构追寻赃物提供了方便。

除了Everledger，还有侧重于药品溯源的BlockVerify，侧重于艺术品防伪的verisart，着力于奢侈品防伪的唯链（VeChain）。唯链由中国区块链初创企业BitSE开发，主要用于LV包的防伪。通过和LV集团合作，在LV包中嵌入NFC芯片，实现LV包每次流转的区块链登记，从而为防伪鉴定和二手LV包交易提供可靠的支持。

当一个溯源区块链登记的标的物是国际贸易货物时，这个溯源区块链就具备了提供供应链金融服务的能力。SKUChain通过在货物包装上装配二维码、NFC芯片或GPS定位设备，使商品的流转能够自动被记录到SKUChain上。同时，通过把银行发行的信用证数字化，使资金流和物流能够同时无缝地在SKUChain上流通。

七、身份认证与公民服务

什么是身份是一个经久不衰的哲学话题。Identity其本意乃是“同一性”，而谈到同一性，不得不提出哲学史上的“忒修斯之船”问题。

一艘在海上航行了几百年的船,被不间断地维修和替换部件。只要一块木板腐烂了,它就会被替换掉,以此类推,直到所有的功能部件都不是最开始的那些了。问题是,最终产生的这艘船是不是原来的那艘忒修斯之船,还是一艘完全不同的船?如果不是原来的船,那么在什么时候它不再是原来的船了?哲学家托马斯·豪倍思(Thomas Hobbes)后来对此进行了延伸,如果用忒修斯之船上取下来的老部件重新建造一艘新的船,那么两艘船中哪艘才是真正的忒修斯之船?

历史上不同的哲学家给出了不同的答案。我更欣赏的一个答案是:忒修斯之船在物理上时时刻刻都不是前一刻的自己,只要时间永远单向流逝,绝对意义的“同一性”并不存在。下一秒的你已经不是绝对“同一性”的你,只是如此近似于上一秒的你,以至于我们可以认为下一秒你仍然会拥有类似的价值偏好,相近的生理反应。语言的抽象和窄域本质导致了我們只能低精度地描述世界,为每一团物质波指定一个身份。

回到现实世界的身份系统。在今天的世界,没有身份就无法拥有银行账户,无法获得社会福利,无法行使受教育的权利,更谈不上参与政治生活。同样,一个区块链上如果用户只拥有匿名的地址而无法证明自己的真实身份,那么其应用场景必然变得狭窄。

ShoCard是一个将实体身份证件的数据指纹保存在区块链上的服务。用户用手机扫描自己的身份证件,ShoCard应用会把证件信息加密后保存在用户本地,把数据指纹保存到区块链。区块链上的数据指纹受一个私钥控制,只有持有私钥的用户才有权修改,ShoCard亦无权修改。同时,为了防范用户盗用他人身份证件扫描上传,ShoCard还允许银行等机构对用户的身份进行背书,确保真实性。

OneName则提供了另一种身份服务。任何比特币的用户都可以把自己的比特币地址和自己的姓名、Twitter(推特)、Facebook(脸书)等账

号绑定，相当于为每个社交账户提供了一个公开的比特币地址和进行数字签名的能力。

一个叫Bitnation的项目则更为激进。用户在其官网上通过区块链登记成为Bitnation的“公民”，并获得Bitnation“世界公民身份证”。然后凭此身份，获得Bitnation自我认可的各种公民服务。

与此相比，爱沙尼亚政府推出的“电子公民”计划可谓真正的接地气。2014年10月，其宣布向全世界开放“电子公民”身份认证服务。任何人只需要在其政府官网填写简单的信息，并用信用卡缴纳50欧元的申请费即可成为爱沙尼亚的电子公民。电子公民可以：①线上登记注册并管理一间基于欧盟商业法律体系的欧盟企业；②获得爱沙尼亚政府认可的数字签名、认证与加密文件的网络服务；③在线开立爱沙尼亚的数位银行账户；④使用全球跨境支付服务。

八、物联网

在即将到来的物联网时代，人们日常生活中的大部分设备将连接到云端网络。设备与设备可以直接通信，而无须经过主人；物联设备可以自主地决定运行的状态，自主地购买服务，自主地完成运行和维护。打印机可以自己订购所需的墨水，空调可以自动调用你的手机导航信息而提前调节温度。但是，传统的物联网模式是由一个数据中心负责收集各连接的设备信息，这种方式在生命周期成本和收入方面有着严重的缺陷。

为了解决这个问题，IBM提出的方案是让未来的每个设备实现自我管理，从而无需经常性地对它们进行维护。也就是说，这些设备的运行环境是去中心化的，它们连接在一起以形成一个持续运行的分布式云网络。只要这些设备都存在，那么整个云网络的寿命就会变得很长，并且

运行的成本也将降低很多。

而解决分布式云网络的一个重要问题就是要解决各节点的信任问题。在中心化的系统中，信任是比较容易的，因为存在一个中央机构管理所有的设备以及各节点的身份，并且可以处理掉不好的节点。但是，如果这对于潜在数量几十亿的上网设备来说，几乎是一个不可能完成的任务。而IBM认为，比特币区块链技术恰恰解决了这个问题。IBM联合三星推出了一个基于区块链技术的物联网概念验证项目ADEPT。

在ADEPT的公开演示中，一台三星W9000型号的洗衣机可以自主地侦测到洗衣粉不足，然后向供应商进行自主订购。根据ADEPT项目的描述，这台洗衣机将能够自行发送更换零配件的订单，甚至能够和扫地机、洗碗机等其他家电设备进行电源竞价，最终实现用户家庭能源消耗的最小化。

同样，在物联网的世界里交易也将会和今天大众普遍理解的交易大相径庭。今天的交易往往是人和人之间的交易，而在物联网世界，交易的参与主体将不再是人，而会是各式各样的设备；交易的金额和频次因此也会发生重大的变化，金额变得极小，频次变得极高。在这样的一个环境下，设备信任网络的建立和微支付都要求我们有一个新的基础架构，而不可能依赖于传统的面向自然人的身份认证体系和面向人际交易的支付系统。

美国一家名为21Inc的创业公司就试图将区块链技术与物联网结合起来。21Inc的愿景是制造出一种可挖比特币的芯片。这种芯片可以安装在任何物联网的设备之中，一旦设备通电，这种芯片就能开始比特币的挖矿工作，挣得比特币。当这个设备需要进行支付时，不再需要人工向此设备充值，该设备可以动用自己挖矿挣来的比特币完成整个支付过程。这个设备就像一个自主系统一样，只要提供电能，就能自我运营。尽管通过这样的芯片进行比特币挖矿的效率显著低于专业的矿机，但是这种自给自足的模式大大减低了人的认知成本。只要插上电源，就可以

不用再管了。这样一个宏大的目标也帮助21Inc获得了高达1.2亿美元的风险投资。

不难发现，这样的技术还可以复制到其他设备上。比如一台饮料自动售卖机，通过卖出饮料获得用户支付的数字货币，当存货不足时，售卖机自动向供货商发出订货单。当供货商补充饮料后，售卖机自动用之前收到的数字货币支付给供货商，并留存利润备用。同样，一台无人驾驶汽车可以成为一个独立自主运营的出租车，向乘客收取数字货币，用数字货币去充电桩购买充电服务，去汽车维修处用留存的利润更换老化的零件。

当然，物联网也不全然是巨头的天下。像Filament、Tilepay，这样的小型物联网区块链初创公司也在进行着自己的探索之路。

Filament正在制造两种硬件设备：Filament Tap，一种能够让物联设备和10英里内的手机、平板或电脑进行通信的模块；Filament Patch，一种用于增强物联设备的互联能力的模块。这些模块会首先被使用在工业设备上，让各个工业设备协同工作，而无需依赖一个中心化的组织者。Filament最近也完成了500万美元的融资。

Tilepay更聚焦于传感器数据的交易上。全球的用户都可以接入Tilepay，提供自己的手机GPS（全球定位系统）、温度计、汽车传感器、可穿戴设备等实时传感数据给数据需求方。数据需求方为自己获得的实时数据支付对应的比特币。Tilepay建立了一个基于区块链的大数据交易市场。

无疑，我们正在迎来一个万物互联、价值互通的时代。

九、保险

当金融证券业在积极探索区块链应用场景的时候，保险业也在紧锣密鼓研究区块链技术，埃森哲的常务董事艾比·让拉（Abizer Rangwala）这样写道：

我认为，保险业正在观察区块链技术，慢慢摸清区块链技术的真正商业用途或者说在一定程度上区块链的实际应用是什么。

区块链技术对保险产品的影响还尚不清晰，相比对银行的影响，可能会需要更长的时间才能显现出来。区块链技术将提高合约执行速度，比如区块链的时间戳特征能够改善个体合同，反映实际风险，如按需车险（合约只在车辆行驶期间有效）。

这样的论述并非空中楼阁。2016年3月，一个名为SafeShares的区块链保险创业公司联合英国老牌保险公车劳合社推出了第一个为共享经济服务的区块链保险服务。这项服务是为一家名为Vrumi的创业公司而量身定制的。Vrumi是一家类似于Airbnb（空中住宿）或Uber（优步）模式的办公空间共享服务平台。每个通过Vrumi提供办公空间的房主只需要缴纳每天2英镑的保费就能成为被保险人，获得75万英镑财物险到500万英镑人身险的完整保险方案。

一般的共享经济都采用所谓“保护伞保险”模式，平台即是投保人，也是被保险人。发生赔付事件时，保险受益人是平台，由平台再赔付给用户。在这个模式下，受损人和保险收益人不一致，而且平台的整体理赔额有上限，一旦到达上限，后续的受损人将无法得到赔付。

与其他共享经济的保险方案不同，在SafeShares这个基于区块链技术的保险方案下，办公空间的提供方是直接的被保险人，拥有直接申请理赔的权利。

区块链+保险领域另一个可能的方向是自动理赔的保险。通过区块链的智能合约技术，保险公司可以无需等待投保人申请理赔，就能主动

进行赔付。例如，可以发行一种基于区块链智能合约技术的航班延误险。通过调用航空公司/机场的公共接口，智能合约得以判断某次航班是否发生了延误，延误情况的严重程度如何，从而自动触发理赔行为，而无需用户主动干预。延误理赔甚至可以用类似出租车打表的方式完成。看着自己账户余额不停地增加，也许延误航班的常客们就不会再爆发国内机场延误时常见的打砸抢式的情绪了。

还有一个可能颠覆今天保险行业的模式是互助保险。互助保险的逻辑出发点很简单，保险本身就是一个互助行为，因此一旦技术允许，我们并不需要一个中介充当组织者，建立资金池，用用户的保费去做各种投资。用户完全可以通过点对点互助的形式，在没有资金池的情况下，通过互助达到保险的目的。2016年5月，美团早期员工创立的“水滴互助”就获得了IDG（美国国际数据集团）、腾讯、真格等机构的5000万美元投资，而其背后就使用了区块链技术。

在荷兰金融咨询机构AXVECO的区块链专家欧利文·瑞肯（Olivier Rikken）的一篇文章中，对基于区块链技术的P2P保险商业模式有过更有趣的模式设计。在Olivier设计的新模式下，保险公司的专业能力将更多体现在匹配供需、风险计算上，而不像今天的保险公司如此注重资产管理能力。

在P2P保险下，保险公司将提供一个保险交易市场，用户可以在市场内提出自己的保险需求，无论是标准化的还是非标准的，保险公司随后通过自己掌握的历史数据给这个保险需求计算出一个参考保费和响应的承保方的预期收益率。随后，想要提供承保服务的用户就可以竞标这份保单，既可以是一对一，也可以是一对多。

区块链在这个市场需要提供两个作用：①对保单交易进行登记；②利用智能合约，在满足赔付条件时，自动从承保人的账户划拨赔款给受益人，而无需银行的参与。在判断是否满足赔付条件时，保险公司可以作为提供损失鉴定报告的第三方。

在这种P2P保险模式下，用于资金端的来源是投资人用户，保险公司可以轻资本运营，甚至这个交易平台可以外包给第三方运行维护。另外，P2P保险由于没有保费资金池，可能在监管上和P2P借贷不需要银行牌照一样而不需要保险牌照，这样就减轻了合规成本。

除了初创公司，人寿保险和金融服务巨头约翰·汉克（John Hancock）也已经开始着手多个区块链概念验证的工作了，其目的在于展示分布式总账技术重塑保险行业的流程。John Hancock正在进行的概念验证项目的合作方是区块链技术公司ConsenSys和BlockApps，项目方向包括“了解你的客户”和“员工奖励计划”等。

另外，除了SafeShares、互助保险、P2P保险的模式，在溯源防伪项目中提到的Everledger也在从防伪的角度切入，和保险公司密切合作提供区块链登记溯源的珠宝盗窃险。看到这么多的保险业的创新火花，我们有理由相信埃森哲的常务董事Abizer Rangwala的看法：“我毫不怀疑，未来几年内，区块链技术将成为在保险业生态系统中的主流技术。”

十、医疗

全球医疗市场大得惊人，仅仅是制药这一个领域，市场规模就高达1.057万亿美元。美国是人均医疗开支比例最高的国家，医疗支出占整个GDP的16.8%，美国每年创造出来的财富中有1/6被花在了医疗上。医疗机构保存了大量的机密信息，例如病史记录、疾病、支付和治疗。区块链技术不仅能为这些敏感数据的安全和隐私存储提供解决方案，而且它还能帮助降低医院和医疗服务者在管理病人和其他信息时的巨大成本。

第一个显而易见的应用场景就是电子病历。在互联网高度发达的今

天，大多数的医院仍然在使用手写病历。这些病历往往如天书般难以读懂，而且一旦丢失或因故无法携带（如出国），再次就诊时就失去了历史可循，甚至可能因此耽误宝贵的有效治疗的黄金时间。中国卫生部早在2010年就签发了《电子病历系统功能规范（试行）》的通知，然而6年后的今天电子病历任然进展缓慢。这其中一个问题就是电子病历的保存是在医院处，而医院却又是医患合同中的利益相关方，大量的医疗纠纷中都牵涉到了电子病历的有效性上。由于医院单方面保管电子病历，在发生医疗事故纠纷时，患者往往指责医院对电子病历进行了修改。

因区块链的不可篡改性和高强度保密性可以给这些电子病历提供一个可靠的访问环境。当电子病历被保存在一个去中心或者多中心参与的区块链上的时候，医院单方面将无法对数据进行任何篡改。而且一旦上链，就可在全球范围内访问数据，无需担心病历丢失或者携带不便的问题，一个人的终生医疗信息都可以被记录在区块链上。位于瑞士的Healthbank(健康银行)就是采用一种完全透明的方法处理医疗信息，用区块链技术为个人医疗数据安全提供保障。Healthbank的口号是“我的数据，我的选择，我的Healthbank”。Healthbank允许个人与患者自己掌握自己的信息。医生访问、睡眠模式、心率、血糖浓度和其他的物联网设备都能够被调查到，并记录到Healthbank的区块链上。

随之而来的是另一个问题：个人隐私的保护。2015年初，美国第二大医疗保险公司Anthem的服务器被黑客入侵，超过8000万的医疗保险客户和员工的资料被盗取。被盗取的个人信息包括住宅地址、生日、医疗身份号码、社会安全号码、邮箱地址和收入数据。就连该公司CEO的个人信息也未能幸免。2015年7月，加州大学洛杉矶分校发现其医疗网络UCLA Health被黑客入侵，又有450万个人敏感信息被盗。究其根本，只要隐私信息依然采用中心化方式保存，就难免发生百密一疏的情况。

区块链恰恰提供了保护隐私的工具。保存在区块链上的病历虽然是在全球任何地方都能访问的，却是用户用密钥掌握数据的绝对专属权与访问权。同时，区块链强大的智能合约功能可以让用户自主的设置权限。比如，用户可以使用这样的智能合约——当自己发生昏迷时，只要医疗机构和自己的亲人同时使用各自的密钥，也能获得访问自己医疗记录的权限。

除了医疗记录，有些创业公司着眼于将区块链技术应用于基因检测数据的共享。成立于2014年的DNA.bits公司，致力于解决针对医疗电子交换法案（HIPAA）的共享基因识别及相关临床数据的问题。由于其产品使用了比特币区块链平台，可聚集来自多个数据源的数据，而无需将这些数据收集到一个中央数据库。

全球医疗市场的几大主要玩家包括诺华制药公司（494亿美元）、瑞辉（474亿美元）、强生（163亿美元）、复迈（118亿美元），巨头间的交叉竞争调用了海量动态医药数据和历史医疗记录，给药物发现和个性化医疗带来高昂的成本。我们可以更进一步设想，如果全世界的医疗记录都加密保存在区块链上，那么只要能设计一种机制，让用户就可以主动将自己的敏感信息清除，而把医疗方面的信息免费或收费提供给医疗研发机构使用。海量、完备的医疗大数据显然将大大加快了研发的进度，为攻克更多不治之症提供帮助。

除了医疗信息与基因检测数据，整个诊疗过程的支付也可以应用区块链技术来提升效率。前面用区块链来管理医疗记录的生命周期的方法，也可以用于管理医疗账单的生命周期。当病患的医疗记录用区块链记录后，自然的医生的处方、诊疗的账单也可以被记录在区块链上。病历、处方、账单都上链后，医院、病患、保险公司这三方也就无需再通过繁杂的申请、核验过程来完成医疗保险的赔付，大大简化了赔付流程，提升了透明度。

Gem是聚焦医疗健康领域的区块链创业公司，其在2015年获得了

700万美元的风险投资。Gem使用多重、硬件安全模块等技术管控区块链上的用户身份和信息安全。2016年4月，Gem宣布与飞利浦合作，推出了Gem Health项目，构建一种能够用来开发企业级医疗应用程序的私有以太坊区块链。对于Gem在管理这种新的私有区块链系统过程中承担的角色，Gem CEO表示他们的目的并不是为了将这个网络“纳为己有”，而是将自己定位为顾问和区块链项目研究公司之间的“红娘”。

另一个区块链医疗领域的初创公司Tierion也在与飞利浦健康开展合作。Tierion聚焦于数据保存方向，除了一般的病历外，其还开发了一种名为Chainpoint的区块链收据标准。任何行业的商家都可以通过此标准来在区块链上签发收据。

十一、博彩和预测市场

博彩与预测市场是区块链的一个重要应用方向。在区块链应用平台以太坊上，预测市场应用是出现频率最高的应用类别。

预测市场（Prediction Market）按照维基百科的定义，是以进行预测为目的而产生的一种投机市场。从发起预测的对象来说其目的是为了预测；从参与预测的用户角度，预测市场可在某种程度上理解成非标准化的博彩。预测市场和博彩的最大区别在于预测市场需要将链下信息进行记录和结果判断。

基于以太坊平台的Augur是目前融资额度最高的区块链预测市场应用，在2015年10月完成了总额520万美元的众筹。Augur目前已经进入Beta阶段，计划将于2016年底前正式运行。截至到2016年5月，Augur在进行Beta测试的阶段中共有618个预测市场项目，其中261个为开放状态，在数量上已经初具规模。Augur相比其他预测市场，其有如下优点。

①无中心化服务器，难以被关闭。传统预测市场一大问题在于扩张到一定程度后容易遭到政治等外力阻碍甚至直接闭站。利用去中心化的区块链技术可以打消该种忧虑。

②用户可以创造自己的交易市场。这意味着预测市场的项目可以是完全自定义而没有门槛。用户可以用此来预测总统大选结果或是明年玉米的收成，也可以是预测一场球赛，甚至明天是否下雨。

③低成本运营，所以低费率。低费率的原因在于运行成本通过区块链分摊，而团队成员在未来也只是通过REP代币而非工资来获取相应收入，所以后续人力成本几乎没有。

④众包型的结果判断。当某个预测项目产生结果时，Augur并不依赖于中心化的网站或个人来判断用户的输赢，即Augur不依赖中心化的信息源来获取美国大选的结果，而是用众包的方式获得大选结果。这避免了中心化信息源的单点故障问题。

⑤安全以及自动化的支付。Augur是基于以太坊的去中心化应用。参与Augur预测市场的用户无需担心对方赖账的风险，也无需担心中间平台卷款跑路。通过透明的开源代码，用户可以有充分的信心预期博弈的公平性。

Augur作为预测市场与博彩类应用的最大区别在于需要进行链下信息的链上录入以及众包式的结果判断。前者更多是利用经济激励实现，后者除了激励以外更多还需要数学模型的帮助。

Augur发行REP作为整个区块链系统的激励代币，对每笔交易收取2%手续费，相比传统预测市场收取5%的手续费更有竞争力。手续费的一半给予流动性提供方，另一半给予合格的REP代币持有者。一方面通过REP可以给予众包的结果判断者奖惩激励，[\[26\]](#)另一方面REP也可以作为Augur团队成员的长期激励因为Augur团队成员持有一定数量的

REP。。故REP更像是Augur这个去中心化区块链预测市场系统的股份。

从“中本聪骰子”到Augur，区块链创业者可以通过数学和博弈制度的设计让古老的博彩和对赌（预测市场）变得更公平、更透明。博彩与预测市场可能无法成为主流，但它们也许会一直存在下去，就像赌徒这个职业一样。

[\[26\]](#) 由于不存在一个中心化的组织，故Augur上所有预测市场结果的事后判断都由REP持有者进行，再通过相应算法确保结果和现实一致。如果没有按时完成对应的项目结果判断的话，REP持有者将失去对应分红。

第六章

从信息互联网到价值互联网[\[27\]](#)

一、技术创新与制度创新

（一）区块链与互联网

区块链给经济社会发展带来了一系列挑战，在明确其技术内涵、路径和应用案例的同时，我们还需要从理论层面和国家战略层面予以进一步剖析和定位，并且从历史演变的脉络中，找到区块链“应运而生”的内在支撑要素。

区块链科学研究所(Institute for Blockchain Studies)创始人梅兰妮·斯万(Melanie Swan)认为[\[28\]](#),

“我们应该把区块链当成类似互联网的事物——一种综合的信息技术，其中包含多种层面的应用，如资产登记、编写清单、价值交换，涉及金融、经济、货币的各个领域，像硬资产（有形财产、住宅、汽车）；以及无形资产（选票、创意、信誉、意向、健康数据、信息等）”，“但是，区块链的概念远不止于此：它是任何事物所有量子数据（指离散单位）呈现、评估和传递的一种新型组织范例，而且也有可能使人类活动的协同达到空前的规模。”

此外，梅兰妮·斯万把由区块链技术带来的各种已有和将有的革新分为三类，即：

①区块链1.0——货币（货币转移、汇兑和支付系统）；

②区块链2.0——合约（在经济、市场、金融全方面的应用，其可延伸内涵远比简单的现金转移要广得多，如股票、债券、期货、贷款、按揭、产权、智能资产和智能合约）；

③区块链3.0——超越货币、金融、市场之外的区块链应用，特别是在政府、健康、科学、文学、文化和艺术等领域。

我们可以看到，区块链虽然源于比特币，但是其应用层面却能够进一步拓展，究其根源，是能够促使当前的信息互联网向价值互联网（图6-1）过渡，为更多领域的金融和非金融创新奠定基础条件。正如德勤亚太区投资管理业主管合伙人秦谊认为：

“区块链有可能颠覆金融行业，重塑如会计、审计等行业操作，并催生新的商业模式；这是一个新的、不断变化的技术，广泛应用于商业还需几年时间。尽管如此，为防错失机会和受到突如其来的科技冲击，各行业的战略家、规划者以及决策者都应该开始研究区块链的应用案例。”



图6-1 从信息互联网到价值互联网

（二）区块链兼具技术与制度创新

1.技术驱动下的金融创新

从技术视角看，我们可以用大数据、云计算、平台经济、移动支付这些通行概念来描述新技术，也可以概括称为ICT。ICT是信息、通信和技术三个英文单词的词头组合(Information Communications Technology, ICT)。它是信息技术与通信技术相融合而形成的一个新的概念和新的技术领域。21世纪初，八国集团在日本冲绳发表的《全球信息社会冲绳宪章》中认为：“信息通信技术是21世纪社会发展的最强有力动力之一，并将迅速成为世界经济增长的重要动力。”事实上，信息通信业界对ICT的理解并不统一。作为一种技术，一般对ICT的理解为不仅可提供基于宽带、高速通信网的多种业务和信息的传递和共享，而且还是一种通用的智能工具。

以ICT为代表的新技术能够改变什么？从宏观看，是经济金融活动的搜索成本、匹配效率、交易费用、外部性和网络效应。从微观看，则是影响企业内部的信息管理、激励约束机制、技术进步和治理环境等。

当前，关于技术对金融的影响，国外最流行的概念就是Fintech（金融科技），即是指伴随着科学技术和管理工作的发展，为了降低金融交易成本、提高金融交易效率而在金融交易手段、交易方法和物质条件方面发生的变化与革新。金融技术创新既是金融效率提高的物质保证，同时还是金融创新的内在动力之一。正是由于科学技术特别是电子计算机技术在金融交易中的广泛应用，才使金融制度与金融交易工具发生了深刻的变化（图6-2）。

应该说，几个世纪以来技术对于金融的影响一直都存在，并非现在才凸显出来。例如，早在19世纪上半期，股票交易信号的传递是由经纪人信号站的工作人员通过望远镜观察信号灯，了解股票价格等重要信息，然后将信息从一个信号站传到另一个信号站，信息从费城传到纽约

只需10分钟，远比马车要快，这一改变曾掀起了一轮小小的“炒股”热。直到1867年，美国电报公司将第一部股票行情自动收报机与纽约交易所连接，其便捷与连续性深刻激发了大众对股票的兴趣。1869年，纽约证券交易所实现与伦敦证券交易所的电缆连接，使交易所行情迅速传到欧洲大陆，纽约的资本交易中心地位进一步凸显。可以说，区块链对金融带来的冲击，首先就是沿着技术演进的路径逐渐发生的，信息技术的发展同样是区块链产生的基础，而区块链技术则进一步推动了金融变革。

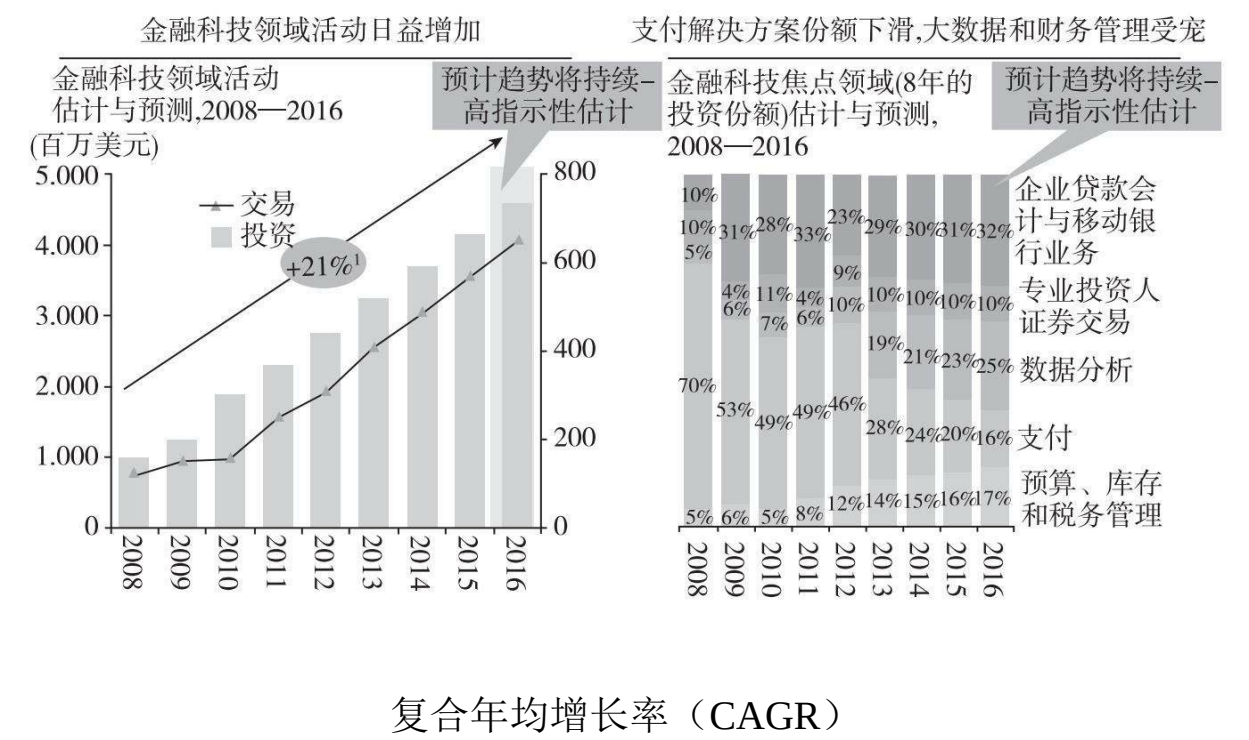


图6-2 全球Fintech的相关状况

资料来源：埃森哲报告：《全球金融科技投资飙升》全球范围（美国、欧洲、亚太）

2.制度驱动下的金融创新

从制度视角看，现代金融改革也离不开制度的优化。例如，从普惠金融到共享金融，更加强调金融发展中的伦理问题，重视制度经济学的影响。近年来，经济金融发展中由于出现了诸多矛盾，因此人们更加重

视伦理学的引入，也就是从伦理方面对经济制度、经济组织和经济关系的一种系统研究。就此角度而言，市场经济和金融运行，它不仅是经济的，更是伦理的。

一方面，我国的金融创新动因，有一些全球性的制度要素，如普惠金融。技术所伴随的机制变革动力，能够对可持续协调发展与实现经济金融伦理作出贡献。例如，在2012年美联储的一份报告中指出，美国消费者中有11%享受不到银行服务（unbanked），另有11%享受的银行服务不足（underbanked）。而伴随着智能手机的普及化，这些人群更容易也愿意运用移动设备来享受电子银行或支付服务。另一方面，还有一些中国转轨期的特有因素。例如，目前很多互联网金融模式就是一种特殊的监管套利创新，是具有短期化特征的。如果利率进入完全市场化状态，金融市场充分竞争，客观地说很多模式的存在空间会进一步缩小，最典型的是货币基金消费支付，像余额宝，欧美货币市场基金的网络化发展轨迹其实已经证实了这一点，当然这只是其中一点，很多现象必须认识到它可能兼具技术和制度因素驱动的特征，所以分析新金融模式必须一分为二来看。

3.区块链兼具技术与制度驱动特征

区块链不仅是一系列新技术应用，更重要的是对制度与规则层面的创新尝试。一方面，虽然人们普遍认为我国的信息技术及其金融应用在很多方面已经居于全球前列，甚至已经开始“弯道超车”，但现实告诉我们这未免过于乐观。例如，国际电信联盟发布的2015年衡量信息社会发展的报告，陈述了2015年度全球ICT发展指数的排名，其中中国位居第82位，较2014年度上升5位。显然，我们的实际技术能力仍然距发达国家很远。就此而言，对区块链的应用，当前各国的差距并不太远。其中，由于金融天然就是基于共享模式，区块链技术则使金融共享的深度和广度空前扩大，更使这方面的应用尝试变得更加重要。因此，积极尝试并探索区块链的应用场景，有助于促使我国综合技术能力在“新平

台”上的提升。

另一方面，技术变革最终还要落到制度变革之上。更具科幻视角的是，当未来技术获得极大变革和突破，以至于从根本上改变人类社会的组织形式、管理模式、信息传递、资源配置时，甚至达到在理想模型中才存在的、稳定有序的、最优的宏观均衡之时，那么货币与金融的存在可能就没有意义了，到此，技术才在真正意义上“颠覆”了金融、“消灭”了金融。在此之前的较长时期内，还需要更多过渡性的改革尝试，目的都是解决现有经济金融运行中存在的矛盾，区块链也给这种制度变革探索提供了一条现实道路。

（三）区块链的价值内涵

在上述分析基础上，我们可以从以下几方面进一步剖析在“互联网+”时代区块链的价值内涵。

区块链是一套特定的规则，即分布式分类总账、智能数据库，或者一套基于网络难以改变的、公开透明的、超大容量的游戏规则。这套游戏规则为什么要改变金融市场中原有的一些规则？无非是因为现有的金融体系中有些规则可能存在瑕疵，即现有规则下的某些金融活动，或者有可能使金融中介部门拥有过强的话语权，或者使企业和居民等个体的影响力过于弱小，以致出现很多问题。例如金融消费者权益保护可能成为全球性的难题；金融创新可能成为少数部门的获利手段；资金配置成本较高，导致融资难、融资贵；信息不对称造成的各种金融服务缺位等问题。而类似区块链的这套新规则可能有助于缓解以上矛盾，使多数人都能够成为规则的参与者和维护者。为此，从规则层面而言，区块链具有重大意义。

首先，区块链价值的真正实现，需要面临以下三方面的挑战。

挑战一是区块链的初始规则如何确立？是依靠大多数投票的相对民

主机制，还是一定程度上依靠线下的公共权威与信用的参与和支持？这是很重要的问题。虽然构建共享共赢式金融发展生态体系，区块链规则具有巨大的发展前景，但与此同时，不能够在初始规则确立时被少数人所利用，并由此非正当牟利。

挑战二是区块链新规则与既有规则的冲突和衔接问题，即如何应对新旧规则的相互适应和改良的矛盾。

挑战三是未来区块链的规则是由网络节点来维护的，但每个网络节点背后都有人的行为，因此，新规则离不开人。如何适应现代金融理论的发展，将人的非理性行为考虑进去，即结合行为经济学和金融学的视角，考虑非正式的规则对一些已有的正式规则的影响，也至关重要。

如果突破了以上三方面挑战，未来区块链这套全新的规则对传统金融市场规则而言，就是很重要的补充，甚至发挥主体的作用。

其次，我们认为，区块链将最先影响到金融基础设施建设，随后扩及一般性金融业务。金融基础设施主要包括核心金融基础设施和附属金融基础设施。按照国际主流概念，核心金融基础设施，又称金融市场基础设施，主要包括支付系统、中央证券存管、证券结算系统、中央对手方及交易数据库等。附属金融基础设施是一个相对广义的描述，主要包括信用体系、法律、会计、反洗钱、信息系统等。

为什么区块链主要影响的是金融基础设施？可以比较的是，过去基础设施都是公共产品，因其成本相对较高、收益较低，为此更多的是由政府、国企等来建设。但现在，在全球范围内，已有大量民间资本逐渐介入基础设施领域，无论是新技术还是新制度规则的演变，都使多元化资本介入基础设施建设的效率大大提高。金融基础设施也面临同样的问题，一些新机制使更多人有可能参与到金融基础设施建设中来，从而既降低成本、提高效率，又保证安全性。

一个直接的案例就是美联储。2015年初，美联储发布了一个提升美国支付体系效率的报告，报告中提及大量利用新技术改善美国支付体系效率的行为。例如，报告提出了一个未来在行业内可推动的方案，即便利金融机构间基于使用通用协议和标准发送和接收支付的公共IP网络直接清算。报告认为，与通过中心辐射状的网络结构清算交易相比，金融机构间基于公共IP网络的信息分布式架构有可能降低成本。因此，美联储欲在中央总账内建立报文标准、通信安全和记录交易的通用协议，以便利相应的银行间结算。同时，还要建立系统规则，保障参与机构能够直接进行实时授权的清算交易活动。由此可见，美联储希望促进这样一套分布式机制的发展，并使其更好地在支付清算体系中发挥作用，且美联储要在其中发挥主导作用。当然，在报告中，美联储还否定了另一方案，该方案是未来其所关注的，但是现在还没有充分引起重视，这就是“数字价值转移工具”，美联储将其定义为银行体系外的一些利用分布式机制进行价值转换的机制。综上可见，美联储高度重视新技术，其更关注的是，在银行和金融机构体系之间如何发挥类似于区块链的这一套分布式新清算机制的作用，同时，美联储本身希望主导这一重大变革趋势。只是现在在金融体系之外，市场自发的价值转换的影响还没有足以使其必须要介入，但也已经充分关注。前者更像是在传统金融支付体系内运用类似于区块链的技术模式。

再次，区块链发展与应用的核心就是登记价值和交易。从长远来看，价值区块链的应用过程是从货币经济学到金融经济学。区块链技术最初源于比特币，是电子货币层面的规则创新。当然，类似的技术也涵盖了其他一些分布式规则的虚拟货币创新。其核心实际上是登记价值与交易价值。区块链这样一套规则有可能更好地从货币层面向金融层面转移，即未来，区块链如何更好地过渡到金融市场层面，这是一个很重要的挑战。区块链技术规则能否影响到资产定价模型？会对金融市场稳定性带来哪些冲击？如何解决金融市场中的非理性繁荣问题？即传统金融市场的短板、内在弊端能否是这样一套东西可以解决的？这些都是值得理论研究者思考的问题。

最后，我们认为，区块链可融合新金融与传统金融间的“代沟”。区块链技术已经开始影响或改变我们的现实生活。目前，有些人在关注，有些人关注还不够。究其原因，除对其内涵认识不足、理解不足之外，还有以下几方面原因。

第一，重大变革对人们脑海的冲击力在弱化。当前，技术变革层出不穷，很多技术变革都是边际上、在潜移默化中影响着人们的生活，很多人对此已习以为常。

第二，这些年来，金融本身一直在异化和扭曲，很多人对金融发展开始变得悲观。新技术能否改变金融存在的问题，从而带来美好社会？很多人对此存疑。

第三，金融的路径依赖性。整个金融（无论国内还是国外）已是“人到中年”，进入一种“亚健康”状态，通过一个“大手术”来解决矛盾是很困难的。如何不断地这个过程中改善体制，利用新技术、新机遇实现共享金融发展是一个重大的挑战。

第四，在商业经济时代，好的不一定是成功的，成功的才是好的，因为对机构和企业而言，短期利润追求才是最大的利益。为此，我们需要有一个更加长远的思路。发展区块链技术不是利用新金融来颠覆传统金融，而是要融合新金融与传统金融之间的“代沟”。

第五，区块链自身还有不成熟的地方，在具体应用模式方面还期待有更加具有突破性的进展。

总的来说，区块链技术并不是凭空出来的“造反派”，它有其历史理论的逻辑过程，核心是引领和涵盖一系列新技术支撑的新规则，使其更好地融入主流，改良现有体系和规则的不足，同时构建一个有利于监管传统金融机构、新型金融组织企业和消费者的共享共赢式金融发展生态体系。因此，需要一方面高度重视区块链技术和规则带来的巨大变革，

另一方面理性看待其面临的风险和挑战。

二、中心化与去中心化

（一）金融的去中心化

1.金融去中心与去中介需区分

我们可以把金融功能和地理意义的中心看作是“大中心”，把金融中介的存在看作是“小中心”。

首先，金融中介一直伴随人类历史发展，比中心的出现要早得多。例如，“银行”（Bank）一词来源于古法语Banque和意大利语Banca，意即早期的货币兑换商借以办理业务活动的“板凳”。银行业也起源于货币经营，早在公元前2000年巴比伦王国的寺庙、公元前500年希腊的寺庙以及公元前400年的雅典、公元前200年的罗马帝国等均有货币经营业的活动记载且十分活跃。

到了中世纪，商品流通进一步发展，欧洲各国贸易集中在地中海沿岸各国，以意大利为中心，因而银行业首先在意大利出现并发展起来。一般认为最早的银行是意大利1407年在威尼斯成立的。其后，荷兰在阿姆斯特丹、德国在汉堡、英国在伦敦也相继设立了银行。18世纪末至19世纪初，银行得到了普遍发展。

金融交易中的信息不对称、搜寻成本、匹配效率、交易费用、规模经济、风险控制等决定了中介存在的必要性。反过来看，金融中介能否真正消失，也要看新技术或制度能否解决这些基本问题。

其次，金融中心化可以包括（无形）权力中心化与（有形）地理中心化。据记载，17世纪时,伦敦的银行收款人,每天去别家银行收取欠它

的现金。一天,两家银行的收款人偶然在一家咖啡馆相遇。他们俩决定当时就在那里核实彼此该收的款项,以节省时间和精力,不久,其他收款员得知了这个办法,均照此办理。从此,这家咖啡馆就成为第一个票据交换场所。各银行负责人发现了此事,有的下令不准这样做,但有些人认为这个方式有价值。后来他们定了一套规章制度,任命了一位经理负责此事,并发展成全世界的票据交换所——伦敦票据交换所。这就是金融基础设施的中心化尝试。

此后,中央银行最早发源于17世纪后半期,以瑞典国家银行和英格兰银行的建立为标志,而中央银行制度的形成则在19世纪初期,主要是以英格兰银行独占发行权为标志,最终建立真正意义上的中央银行制度是在20世纪初,主要是以美国的联邦储备系统的成立为标志。由此,现代意义上的金融中心化机制得以建立起来。同时,金融也在空间地理意义上进行集聚,如17世纪出现历史上第一个真正意义上的国际金融中心阿姆斯特丹。

我们看到,金融中心化的过程要晚于金融中介的出现,这就意味着在历史上曾经很长一段时间都有非中心化的状态与过程。历史的演变是逐渐波动的。这样就产生一个问题:短期和长期这种中心与中介的“去”会产生什么样的现象?

从形式上来看,去中心在短期内更容易实现,因为原有的中心在弱化。各个国家央行的控制力在迅速弱化,传统意义上的很多中心概念在新的网络时代也变得不一样了。金融的资产端、资金端、交易端都发生了一些变化。然而,这是否意味着传统的伦敦、纽约这样的国际金融中心发生了根本性的变革?从短期来看,去中心化比较容易;但从长期来看,本质上的去中心依旧是比较困难的。除非颠覆现有的社会权力架构和组织形式,否则真正的长期去中心化只能是空谈。

从长期来看,去中介似乎更容易实现。虽然短期内由于有很多伪中介,导致去中介比较难。但最终来看,金融演进的逻辑无非是利益、效

率、安全的“三角制约”，主要技术的挑战都在于对这三个矛盾的权衡。

而当前，从技术视角看，我们关注的是为什么金融更可能去中心、去中介？从制度视角看，则需考虑为什么金融需要去中心、去中介？目前的中心化和去中心、中介化和去中介，不是简单快速地就从一个极端到另一个极端，历史的演变在很长一段时间对此是纠结的。

2.现实中的挑战与局限性

在现实中，中心化与去中心、中介化与去中介往往都不是单向变化的，而是充满了不确定性与多元性。我们可以从以下方面来分析其复杂性。

第一，真正的去金融中介（小中心）能否实现？

首先，以经常被看作是去中介代表的P2P网贷为例，实际上在国外，对冲基金和银行正在大张旗鼓地进入P2P领域——不仅通过证券化把P2P贷款重新包装为新的金融工具，还通过这些平台从事贷款业务。英国《金融时报》专栏作家吉莲·邵蒂撰文提出这是源于一个卑鄙的动机：监管套利。她在文中提到，纽约一名银行高管最近在一次会议上（带点不好意思地）解释称：“我们喜欢P2P，因为我们在那里可以做一些我们在银行没法做的事。”

近年来，鉴于个人借贷或投资者发挥的作用逐渐变弱，而包括对冲基金和银行在内的大型机构则逐渐成为游戏主角。国外一些典型的大型P2P网贷平台也在考虑放弃“PEER”的提法。例如，美国最大市场贷款平台贷款俱乐部总裁瑞纳德·兰普（Renaud Laplanche）曾建议将行业名称改为“市场贷款”。《纽约时报》此前借用了第二大贷款平台Prosper Marketplace总裁对该行业的另一说法——“在线消费者金融”。实际上，作为P2P网贷典范的Lending Club来说，显然其典型业务模式也距离P2P甚远（图6-3）。

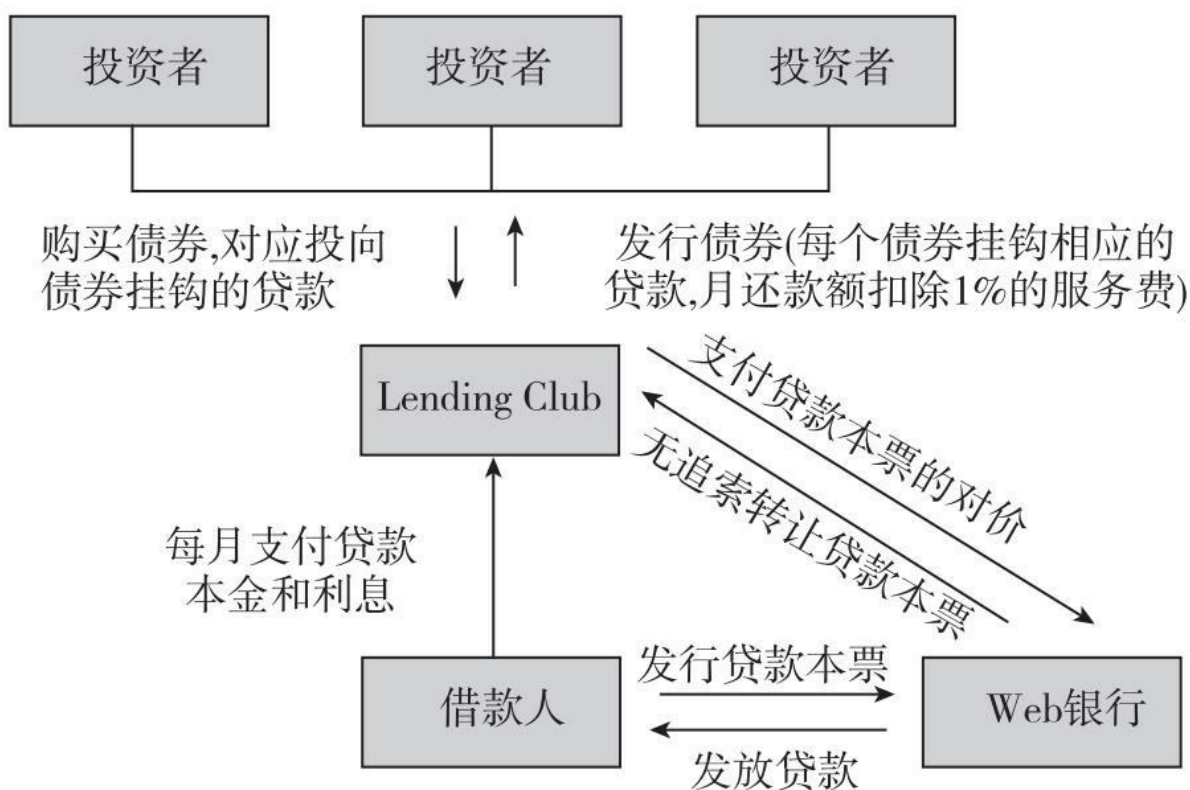


图6-3 Lending Club的业务流程

其次，就股权众筹来看，值得注意的是，目前众筹融资中的一个重要趋势就是采用“领投—跟投”模式，利用专业的领投人来进行项目筛选和风险控制，因此它更像是将传统金融中介的功能蕴含在新的投资者结构当中，而不是简单地“去中介化”。

最后，就银行业来看，美国的富国银行有6200家网点，这个数字在过去三年基本上没有变化。许多银行过去都讲过要进行银行业务网点调整，减少网点。但美国联邦储蓄保险公司的数据表明大银行业务网点并没有减少，相反在城市中心还有所增加^[29]。一方面大家都认为互联网的兴起会减少人们对银行网点的需求，而另一方面许多大银行并没有减少网点。

第二，金融基础设施领域的中心化（大中心）表现（央行主导

权)。

一方面，以支付清算基础设施为代表，在反思2008年金融危机之后，2012以来中央对手方清算机制（CCP）快速发展起来。该机制最早起源于场内衍生品交易市场。伴随着场外金融市场的发展，采用CCP可以有效降低对手方风险，促进市场交易活跃，有效管理系统性风险；从微观角度来看，净额轧差还可以显著提高资金使用效率，降低市场参与者的参与成本。金融危机以来，CCP在化解系统性风险方面的作用得到了充分发挥和高度重视。这确实是典型的中心化机制体现。另一方面，以区块链为代表的分布式支付清算机制，不仅在现实中促进了市场主体的积极参与，而且也引起了各国监管者的高度重视，这与CCP类似的中心化机制采取了截然不同的技术路径。

同时，就货币层面来看，由央行中心化的发行，也不是“与生俱来”的。在历史上的很长一段时间内，货币都是“非中心”的。20世纪中后期兴起的新货币经济学则认为，现有的货币、金融体系并非自然演进的，而是法律限制或政府管制的必然结果。在自由放任的竞争性市场条件下，不一定存在集记账功能和交换手段两大职能于一身的货币，货币现有的两大职能将由不同的物质分别承担，市场中以货币为媒介的交换最终将被“精密的物物交换”所取代。可以看到，电子信息技术演进带来了货币新的“去中心化”的动力。

第三，如何看待地理意义上的中心化与去中心？

金融地理学(Financial Geography)作为近年来兴起的一门边缘学科，它的最大贡献是提供了研究金融问题的全新视角和方法论。进入20世纪90年代以后，很多经济学家认为由于IT技术的发展等，地理因素已经不重要，典型代表如奥·希林(O'Brien)提出的“地理已死”(end of geography)。我们需要思考的是，伴随着网络化、智能化时代的来临，传统空间地理意义上的国际金融中心会不会逐渐被弱化甚至消亡？

（二）区块链的去中心化

我们之所以进行上述讨论，并非是显示出对去中心、去中介的悲观态度，而是强调这些变化可能是多向的，在当前走向去中心的大趋势下，可能存在多向演变和阶段性波动。如果用“去中心化”来涵盖去中心和去中介两个概念，可以得出以下结论：在可预见的未来，可能不是金融完全去中心，而是多中心（小中心）与弱中心（大中心）。

区块链的探索道路也不是简单的去中心，而可能是多中心或弱中心。现在市场谈论较多的“去中心”，其最终结果更可能是多中心，从而弱化少数中心话语权过强所导致的规则失控。当万物互联使所有个体都有可能成为金融资源配置、金融产业链中重要的中心节点时，或许就实现了最理想的市场状况，使传统金融中介的中心地位发生改变。这种改变不是说传统金融完全被革命、被颠覆，而是从垄断型、资源优势型的中心和强中介转化为开放式平台，成为服务导向式的多中心当中的差异化中心，从而使传统中介中心和新的中介中心获得共赢，在一个共享共赢的金融时代获得一种新的发展定位。

值得关注的是，2008年危机之后，早期的华盛顿共识走向了失败，出现了大量的中心化趋势。有的希望通过中心化来解决金融政策和交易效率，有的希望通过中心化机制来解决系统性金融风险。所以，当前市场面临的一个重要挑战实际上就是“中心化”与“弱中心”的挑战。

区块链带来的多中心和弱中心能否解决相应的2008年危机所昭示的效率和风险的矛盾？能否改变现代金融体系的内在脆弱性和创新失控等问题？作为研究者，目前我们非常有信心，这种信心来源于对理论内涵和逻辑线索的把握。但与此同时，这种变革并不是轻而易举的，它需要在实践层面有更深入的研究和探讨。因为当前的时代正是一个中心化与去中心都非常突出的矛盾冲突时代，现代共享金融则可以实现二者融合，也可以努力用区块链的技术来解决传统中心化难以解决的矛盾。

回顾历史，展望未来，基于中国古代的阴阳五行理论，可以看到金融发展中需避免“过犹不及”，而中心与去中心，也是“合久必分，分久必合”的关系。当前，长期中心化金融模式的弊端逐渐显现，历史“天平”开始向“去中心”一方偏离，当然这一过程可能是长期的。

区块链能够遏制传统“中心化”模式下的“短板”，也是为了达到罗伯特·希勒在《金融与美好社会》一书中所描述的目标。希勒教授是理想主义者，他相信人性的光辉。“通过技术安排为公众的利益重塑金融业，把金融业作为人类财富的管理者；通过公众的广泛参与，让金融业为人类社会的良性发展服务。全民的广泛参与也会打破金融的精英权力结构，使金融民主化，并实现财富分配的公平。”国际货币基金组织副总裁朱民这样总结《金融与美好社会》一书作者罗伯特·席勒的理想。所有这些都可以通过区块链的非中性化模式来设计，促进更多主体（节点）的参与及金融话语权提升。

如何探索出一条通往“金融与美好社会”的梦想之路？共享金融自诞生之日起就被寄予了厚望。作为共享金融重要抓手的区块链技术，实际上代表了去中心化的机制，无疑能够为人类迎接“金融与美好社会”提供最好前景。

最后，还需要注意的是，区块链带来的金融创新与去中心化不等于全民搞金融，因为当大量游离于监管之外的“灰色金融”泛滥，或者弱势群体通过“过度负债”来消费和投资，同样会带来巨大的系统性风险。

三、区块链与共享金融

（一）共享经济

2015年10月29日闭幕的中共十八届五中全会首次提出“创新、协

调、绿色、开放、共享”五大发展理念。其中“共享”发展理念主要是突出人民主体地位，强调必须坚持发展为了人民、发展依靠人民、发展成果由人民共享，做出更有效的制度安排，使全体人民在共建共享发展中有更多获得感。

经济共享发展的理念一直贯穿在经济学演进与各国实践中。早期的共享经济理念主要针对市场经济国家快速发展中的收入分配矛盾，试图通过优化和完善分配结构，从根源上解决现代资本主义的某些失衡，缓解日益凸显的各阶层利益冲突。进入21世纪之后，互联网信息技术深刻改变了经济与社会组织结构，对信息采集、处理、交换产生了深远影响，对诸多行业的生产与商业模式产生了冲击。这不仅使剩余资源的使用效率、使用方式变得更丰富，抑制了资源价格的过度膨胀，同时也使消费者主权得到进一步提升，通过“使用权”而非“拥有权”的交易，就能够更好地享受经济发展的成果。

2016年政府工作报告中也指出：“支持分享经济发展，提高资源利用效率，让更多人参与进来、富裕起来；要推动新技术、新产业、新业态加快成长，以体制机制创新促进分享经济发展，建设共享平台，做大高技术产业、现代服务业等新兴产业集群，打造动力强劲的新引擎。”

从根本上看，共享经济是技术进步的结果，共享经济产权层面的特点是所有者暂时让渡使用权以获取收入的租赁经济，但是这种经济模式在互联网时代以前没有形成气候。云计算、大数据、物联网、移动互联网（云大物移）大大降低了租赁交易的信息成本，减少了信息不对称，使原本不可能达成的租赁交易成为可能。可以说，共享经济模式带来的最大好处包括更节约的时间、更优化的资源配置和更灵活的就业。

当然，一方面，共享经济给消费者和直接从业者带来了实惠（除了收入，还有更多的从业自由），有人认为它的发展空间很大。《零成本社会》的作者里夫金(Jeremy Rifkin)指出共享经济是一个方兴未艾的新体系，并预测共享经济将颠覆许多世界大公司的运行模式。另一方面，

共享经济挑战了传统商业模式以及现有制度安排，可能损害既有从业者利益，继而引起一些社会问题。

可以预期的是，共享经济将快速改变大量现有行业，例如快递业、家政服务业、教育行业、培训业、个人服务业、新闻业、租赁业、广告创意业、医疗业、个人旅游业、宠物寄养业、社区养老业等。

（二）共享金融

所谓共享金融，就是通过大数据支持下的技术手段和金融产品及服务创新，构建以资源共享、要素共享、利益共享为特征的金融模式，努力实现金融资源更加有效、公平的配置，从而在促使现代金融均衡发展 and 彰显金融消费者主权的同时，更好地服务于共享型经济发展道路，进而促进经济社会的创新、协调、绿色、开放型发展。

共享金融发展的基本动力，包括技术（新的信息技术+新的金融技术）与制度（新的正式规则+新的非正式规则）。这两大核心要素和基本动力，既带来了全新的金融创新模式（自金融模式），也引起了对传统金融的改革与完善，更有二者的融合式创新。

值得注意的是，无论从技术还是制度来看，互联网金融体现出的都是共享金融的核心理念。时光向前追溯，早期促使金融得以变革的技术与互联网无关，可能是电报、电话等，而源自草根的金融萌芽却一直带有互助共享的色彩，直到被大资本的贪婪所淹没。未来的物联网可能替代当前的互联网形态，主流的信息技术也可能发生难以想象的演变，但是金融发展目标，仍然是如何进一步在金融运行中体现出个性与民主，遏制金融巨鳄的“丑恶”与金融面纱的“虚妄”，在决策共举、各方共赢、利益共分、机制共建、风险共担、事业共助的基础之上，构建真正有利于美好社会的“好金融”。由此来看，即便互联网金融一词终将消逝在历史长河之中，共享金融的生命力也能够伴随金融理性、道德、自律的成长而延续下去。

（三）区块链助力共享金融

作为一种去中心化的机制和信用共识机制，区块链有助于推动共享金融的模式不断扩展和演变，从而推动整个现有金融产业链的不同层面都能够进一步实现资源的共享、共赢发展。

展望未来，区块链技术所助推的共享金融应该呈现如下发展路径。

第一，金融终端的资源与功能共享。从国家资金流量表（金融交易）来看，在非金融企业、金融机构、政府、住户这四大部门中，其中住户部门是典型资金净流出，也是金融资源交易链条的起点。在主流金融运行模式下，住户资金只能通过间接融资市场（银行为主）、直接融资市场（股票和债券市场为主）、结构性融资（复合型的证券化产品）等，进入到一国的“金融血管”之中。在此过程中，住户部门往往缺乏有效的话语权，只能作为金融机构“厂商”的“原材料”提供者。在区块链推动的共享金融发展模式下，首先意味着作为金融产业链上游的住户部门，应该在金融产品和服务的提供中发挥更大的作用、拥有更高的地位。因为住户部门可以借助于互联网技术、开放的平台、众律性的规则，低门槛地直接成为金融资源的供给者，使金融产业链进一步“前移”，从而对主流金融部门的“谈判权”形成制约。对住户部门来说，这实现了与金融部门的责权“共享”。

第二，金融媒介与渠道的共享。互联网的发展带来了一个全新的大平台经济时代，平台的参与主体越多，对供给、需求、中介各方的利益和价值就越大。平台经济的开放特征与传统金融部门的封闭式发展，本来就形成了鲜明的对比。平台经济与金融的发展恰恰反映了共享金融的核心思想。一方面，传统的金融与非金融部门的边界进一步模糊，主流金融机构面临更加明显的“脱媒”，越来越多的主体参与到金融产品与服务提供中，成为重要的金融资源流转中介。另一方面，越来越多的“金融厂商”转换成为“金融平台服务商”，平台经济效应使“自金融”模

式在效率和风控上成为可能。所有这些变化虽然仍处于萌芽阶段，但是对于传统金融中介与新兴金融中介围绕渠道的共享，对于金融供给者、需求者、中介依托合作平台的共享，都提供了令人振奋的发展基础。

第三，金融消费与需求的共享。对于金融消费和需求来说，面临的是日益复杂多样的金融产业链，而新技术和制度变化将有助于其“拨云见日”，更充分地参与到金融运作之中。一是对于需要金融资源流入来维持的企业部门来说，其中的小微企业是最为“饥渴”的需求者，有限的金融资源支撑着其在就业方面的巨大贡献。共享金融的理念和模式必须着眼于为其创造可持续的金融“输血”模式。二是金融资源的流动并非单向，而是双向甚至多向，在众多维度上同时交织在一起。例如，居民也是消费金融的资金需求者，企业可能是资产管理的资金供给者，在此过程中，既需要着力实现不同角色功能的共享与转移，也应促进以共享理念来提高不同定位中的企业和居民对于金融中介的“谈判权”。三是推动金融创新更加重视需求导向，在技术可行的支持下，实现“流水线”式的标准化“金融快餐”与“口味各异”的“金融风味小吃与大餐”并行发展。

第四，金融风险与监管的共享。一方面，现代金融体系之所以存在许多功能缺失，原因之一就是风险的不可控或弥补的高成本。例如，在小微金融和普惠金融领域，信息的不确定、信用基础的缺乏等加重了金融服务困难，而如果实现不同组织与主体的信息系统交互、风险合理共担，则有助于介入那些传统的金融“空白区”。再如，系统性风险与非系统性风险的边界，其实并没有教科书中那样分明，在“动物精神”与“冰冷技术”共存的现代金融市场上，风险预期提升、普遍恐慌、羊群效应、以邻为壑等现象的存在，都容易助推风险的积累。由此，随着新技术使得微观金融行为的甄别能力上升及不确定性分析的越加准确，通过某种技术与制度安排对风险进行合理分担和分散，而非“游牧民族”式的驱离或被投机利用，则成为区块链式共享金融有助于金融稳定的重要尝试。另一方面，区块链技术与规则的探索可以推动社会信用体系的完善，尤其是对于难以进入到传统金融体系来积累信用的主体来说，介入

共享金融实践可以为其创建金融信用基础。同时在“人人参与”的新模式中，自律与他律成为能否继续参与的前提，这也使传统金融监管难以覆盖的“盲区”受到公共金融规则的约束，从而实现新旧监管模式的共存。

第五，金融与实体的共享式发展。无论在经济上还是统计意义上，金融与非金融部门在本质上就是相依相存的，金融部门的利润很大程度上是与实体部门交易完成的，只是随着金融部门权力的扩张和衍生金融产品创新失控，才出现了某些“自我游戏”式的交易。区块链助推的共享金融模式，强调的是与实体部门的共赢发展，包括使多数微观主体充分分享经济增长与金融发展的成果；有利于实体部门规模和结构的完善，而非强化已有的矛盾；避免内部结构失衡和金融创新的失控；解决好金融部门与实体部门之间的分配问题；减少行政性干预，强调市场化运行机制和自律环境优化。综上所述，在全新的共享金融理念的引导下，现代金融发展将从“脱实向虚”转向“以实为主、以虚为辅”。

四、区块链与货币创新

（一）无现金社会

当前，随着互联网时代的技术进步不断推进，作为金融基础设施重要组成部分的支付体系正在发生着根本性变革。

在世界各国，当前现金使用比率的下降，确是不争的事实。其根源还是电子支付、电子货币带来了更高的效率和更低的成本，当然也有助于“魔高一尺、道高一丈”的违法追踪与风险控制。根据可得到的最新数据，凯捷(Capgemini)与苏格兰皇家银行集团(RBS)联合发布的《2015年全球支付报告》显示，2014年非现金支付交易量增速预计达到8.9%，高于2013年的7.6%，创下3897亿美元的交易量新高。另据国际清算银行(BIS)统计，2014年19个最大经济体的流通中现金余额为国内生产总值

(GDP)的7.9%，2010年则为8.4%。

目前，我国的非现金支付增速业已居全球前列，近年来银行和非银行支付机构的电子支付业务较快增长，其中，由于网络经济的快速增长、智能手机用户数量的大幅提升，使我国成为全球范围的移动支付高速增长区域，也是新支付技术的实践“热土”。例如，2016年2月18日苹果公司Apple Pay移动支付服务正式登陆国内市场，引起了业界、媒体和“果粉”们的热议。

对此，一方面，从需求角度看，老百姓更加适应非现金的电子化支付模式的运用，因为网络购物、线下电子支付场景正日益完善。另一方面，从供给角度看，新兴电子支付技术已经更加成熟，各类机构不断推出效率与安排相协调的支付工具与方式。

根据央行统计，2015年，全国共办理非现金支付业务943.22亿笔，同比增长50.4%，增速较2014年提升25.29%；共处理金额3448.85万亿元，同比增长89.76%，增速较2014年提升76.71%。在非现金支付中，电子支付尤其是移动支付业务保持快速增长，非银行支付机构发展势头迅猛。2015年，银行业金融机构共发生电子支付业务1052.34亿笔，金额2506.23万亿元。其中，移动支付业务尽管总体占比较小，但发展速度较快，2015年全年发生业务138.37亿笔，金额108.22万亿元，同比分别增长205.86%和379.06%。2015年，非银行支付机构累计发生网络支付业务821.45亿笔，金额49.48万亿元，同比分别增长119.51%和100.16%。

无论在发展中国家还是发达国家，新兴电子支付不仅能够替代纸币的支付功能，而且能够依托支付渠道解决弱势人群的金融需求。例如，肯尼亚M—Pesa手机银行的出现，使移动业务与家庭汇款等基本金融需求密切结合起来，充分体现了移动支付的高效率和低成本，较好地满足了落后地区的支付需求。再比如，美联储在2012年发布的报告就表明，在美国的消费者中还有大约11%的人无法享受到银行服务，另有11%的人只享受到较低水平的银行服务，而与充分享有银行服务的人相比，这

些人往往属于弱势群体，但他们却多数都拥有智能手机，并且也愿意使用移动银行和移动支付。由此来看，在我国，除了城市的中低收入人群，广大农村领域也应是以新兴电子支付来践行普惠金融的重要试验田。

在政策支持和科技进步驱动下，似乎全球都不可避免地要从现金走向电子支付。2013年挪威学者纯德·艾德森（Trond Andresen）就在一篇工作报告中指出，“实物货币的必然消亡只是个时间问题”。当然，这一过程可能是漫长的，因为纸币仍然有其需求空间。例如据统计在美国，50~100美元的交易只有16%用现金，而1美元以下的交易则有66%以现金完成。由此来看，无现金社会也需要支付习惯的转变，以及电子支付真正在低成本、便利与安全之间做到极致。

（二）数字货币支付

电子支付的变革与货币形态的变化也是密不可分的。此前，央行召开数字货币研讨会，周小川行长也就此接受了采访。数字货币这一公众相对还较陌生的概念，迅速引起了各界的关注和热议。实际上，虽然近年来数字货币已经成为业内流行的全新概念，但迄今为止还没有统一的内涵边界。

如果要追根溯源，则需从电子货币的概念着手讨论。根据巴塞尔银行监管委员会（BCBS）的定义，电子货币是指通过销售终端、设备直接转账或电脑网络来完成支付的储存价值或预先支付机制。国际清算银行（BIS）早在1996年就开展了一系列研究，并认为电子货币可能会影响到中央银行的货币政策，如影响央行控制的利率和主要市场利率的联系。

客观来说，一方面，长期以来央行依然具有垄断性的货币发行权，同时也基本掌控着主要电子货币的发行权；另一方面，电子货币也给货币政策理论框架带来了很大冲击，因为“货币”的可控性、可测性、相关

性都在发生变化。当然，随着新技术日新月异的变化，逐渐出现了可能脱离央行控制的新兴网络电子货币形态。在新技术的冲击下，究竟什么是“货币”可能越来越说不清楚了，其概念、范畴、转移机制都在发生变化。其中，大额与小额、银行与非银行、中心与去中心产生了不同形态的货币及货币转移带来的深刻影响，这体现为对货币数量、价格、货币流通速度、货币乘数，以及存款准备金等制度的冲击。

进一步梳理电子货币的发展脉络，需要从货币背后的信用最终支撑入手。

第一，最为典型的法定电子货币的信用支撑，或者直接来源于各国央行，或者是由银行业机构提供直接支持，央行依托委托—代理关系给予间接信用支撑。以信用卡为代表的传统电子支付创新，以及金融机构电子钱包的出现，实际上都属于货币的形态和体现发生了变化，但没有跳出央行信用直接或间接的覆盖范畴。

第二，伴随着电子商务的发展，越来越多的非银行机构介入电子支付工具中，也对货币结构和范畴带来了新的影响，其信用最终性支撑与央行的联系变得更弱一些，因此成为各国监管的重点。如欧盟专门制定规则，用以规范在信用机构之外发行以电子货币为支付方式的企业或任何法人。

第三，在多元化的网络经济时代也出现了由某些“网络货币发行主体”提供信用支持的虚拟货币。如果这些虚拟货币最终用于购买程序开发商所提供的电子产品，则交易中真正发挥媒介作用的是现实中的货币，虚拟货币并未形成独立的电子货币。如果虚拟货币不是从程序开发商中兑换获得、且交易对手不是货币发行方（程序开发商），那么这种虚拟货币就可能独立地在虚拟世界里执行其商品媒介的功能，如游戏玩家间在淘宝网上用人民币交易某种游戏币。当然由于规模通常较小，其对现实经济的影响并不显著。

第四，20世纪80年代，一批国外专家开始研究基于特定密码学的网络支付体系，并且探讨了匿名加密货币，由此出现了作为电子货币高级阶段的、新型数字货币的萌芽。到2008年中本聪发表论文描述比特币电子现金系统，2009年比特币诞生，使我们对数字货币探索到了新阶段。当然，目前数字货币多少都存在各种缺陷，比特币的资本属性也似乎多于货币属性，并且常常陷入炒作带来的价格波动中。

总的来看，严格意义上的数字货币属于最后一种，更多开始依托以区块链为代表的分布式规则、智能代码来发行和运行，其信用支撑距离央行的中心化机制越来越远，虽现在规模尚小且技术还需成熟，但未来对现有货币机制可能带来重大影响。对于数字货币与区块链的关系，需要从不同角度来看，例如当我们谈到比特币时，它实际由区块链底层技术（协议与客户端）和现实存在的加密数字货币组成。依托于区块链或其改良技术，也出现了其他一些类似比特币的虚拟货币。此外，虽然是当前最典型的技术，但数字货币的底层支撑不一定限于区块链，同时区块链也可以进一步拓展到货币之外的各类去中心化价值交换活动。

因此，当我们谈到数字货币的时候，一种强调的是新型的电子货币，可以利用加密技术实现独立于中央银行之外，按照特定协议发行和验证支付有效性；另一种则是对现有电子货币典型模式的进一步优化，从而既引入包括赋予货币智能合约之类的新技术支持，又保持央行对货币运行的适度控制力。就我国央行来看，短期内应该更为关注的是后者。

从现金到非现金支付、从传统卡基电子支付到网基电子支付、从简单电子形态支付到智能代码支付、从支付工具层面到货币层面，应该说新技术在不断改变着货币金融体系。最终有可能带来更高的交易效率、更低的成本、更精准的政策执行、更有效的反洗钱等风险控制，从而深刻改变着老百姓的生活，并使我们有在全球货币体系变革中争取更多话语权。当然，这些目标并非轻易能实现，夸大或低估其影响都是不

理性的，还需大量的研究探索，专业的普及与公众教育，从而“挤出”数字货币领域的违法者、投机者与行业“劣币”。

五、区块链与金融创新

除了数字货币之外，区块链的其他金融应用也有广泛的前景。例如在支付清算基础设施领域，SWIFT作为一个链接了数万家银行的通信平台，已经被新兴崛起的区块链技术所威胁，一些区块链初创企业和合作机构开始提出一些全新的结算标准，如R3区块链联盟已经制定了可交互结算的标准，截至目前，全球已有近50家大型银行和金融集团加入了R3。

（一）金融应用领域

如在资本市场方面，据华尔街日报于2015年11月报道，世界上一些最大的交易所、银行和交易服务公司已联合成立了一个跨行业集团，命名为“交易后分布式总账工作组”，探索区块链将如何改变证券交易结算方式。参与机构包括伦敦证券交易所、伦敦清算所、芝加哥商品交易所、瑞银集团以及欧洲清算中心。区块链可以创建一个开放式、防篡改的交易总账，它可能取代并简化证券交易中许多复杂的系统。任何类型的金融资产，比如债券或者股票，都可以转变成编码，通过区块链来完成传输交易，而无须到清算所。这意味着股票交易结算过程可能在几分钟内能完成，而不需要耗费两三天的时间。此外，纳斯达克（Nasdaq）总裁兼首席运营官弗里德曼在2016年4月表示，区块链技术可以让金融机构例如纳斯达克追踪到任何资产类别的最终所有者。纳斯达克在世界范围内向超过100个地区的交易所和清算机构提供技术支持，公司正在与客户讨论区块链技术以及它的潜在用途。她认为，在纳斯达克的技术空间里，区块链可以缩短结算时间以及释放银行中的资本，区块链技术有发展的潜力，但是需要一点时间。

区块链还可以应用到票据领域。票据是一种有价凭证，其在传递中一直需要隐藏的“第三方”角色来确保交易双方的安全可靠。比如在电子票据交易中，交易双方其实是通过人行ECDS系统的信息交互和认证；纸质票据交易中，交易双方信任的第三方是票据实物的真伪性。但借助区块链，既不需要第三方对交易双方价值传递的信息做监督和验证，也不需要特定的实物作为连接双方取得信任的证明，实现了价值在点对点之间的“无形”传递。另外，在实际的票据交易中，经常会有票据中介这一角色利用信息差撮合，借助区块链实现点对点交易后，票据中介的现有职能将被消除，并以参与者的身份重新定位。[\[30\]](#)

再者，区块链有助于金融信用体系建设。目前，商业银行信贷业务的开展，无论是针对企业还是个人，最基础的考量是借款主体本身所具备的金融信用。各家银行将每个借款主体的还款情况上传至央行的征信中心，需要查询时，在客户授权的前提下，再从央行征信中心下载参考。这其中存在信息不完整、数据不准确、使用效率低、使用成本高等问题。在这一领域，区块链的优势在于依靠程序算法自动记录海量信息，并存储在区块链网络的每一台计算机上，信息透明、篡改难度高、使用成本低。各商业银行以加密的形式存储并共享客户在本机构的信用状况，客户申请贷款时不必再到央行申请查询征信，即去中心化，贷款机构通过调取区块链的相应信息数据即可完成全部征信工作。[\[31\]](#)

最后就保险方面来看，基于区块链的风险管理模型，可能包括自我管理或风险管理协议，点对点保险平台，以及充分的资金解决方案。应该说，近年来国内大力推动的相互保险，实际上就与区块链技术有天然的联系，因为其具有安全性、信任、交易更直接、效率等保险业需要的基本特质。2015年底，劳合社（Lloyd's）在伦敦举行研讨会，强调将区块链及其他技术应用到保险市场，并将其作为现代化计划——目标运营模式（Target Operating Model, TOM）的一部分。劳合社运营总监思瑞·坎瑞（Shirine Khoury-Haq）在一份声明中提道，区块链技术有望增加保险市场的风险记录能力、透明度、准确度以及速度。埃森哲的常务董事

艾比译·让拉（Abizer Rangwala）指出：“保险业正在观察区块链技术，慢慢摸清区块链技术的真正商业用途或者说在一定程度上区块链的实际用例是什么。毫无疑问，未来几年内，区块链技术将成为在保险生态系统中的主流技术。”

（二）应用前景分析

当前，IBM、摩根大通和其他一些大机构以及美联储为什么要重视区块链这套分布式的去中心机制？它们不是要为自己培养一个完全的颠覆者，而是希望把握未来的不确定性，在这个新的机制中掌握一定的话语权。

如果传统（金融）机构做的是规则1.0，互联网（金融）企业是2.0，那么区块链就是3.0，2.0的互联网（金融）企业对于区块链不积极，因为它们正处于赚钱比较容易的黄金时期，并且本质上还是一种中介化的替代机制，对于大数据的集中掌控；1.0的传统金融机构更积极，因为它们的竞争压力更大，在2.0的竞争中已经落后，还不如直接跳到3.0的竞争。但是，历史上的转换值得我们思考。技术的快速变革令人惊讶，从一代到下一代的迭代似乎瞬间就可以完成。正如过去人们不相信人工智能可以打败世界顶尖围棋手，但当“阿尔法”赢了李世石，人们仿佛突然发现一系列技术革命的“火车”扑面而来。而当你认识到技术来到眼前的时候，它其实已经离你远去了。这就是新技术的挑战值得我们敬畏、探讨的原因。

总而言之，我们需重视区块链和数字货币的巨大挑战，但不应神化！区块链的生命力在于开启了冲击既有僵化体系的“潘多拉之盒”。但在初始阶段，除了理念转变与宏观把握，最需要的是专业技术人才的培育、应用技术的拓展与实践项目的落地。

此外，由于这个领域是跨界的，只了解程序而不了解技术是行不通的，只了解金融不了解技术也会面临挑战。但是也不要什么东西都装

进去。无论中心化还是去中心，背后都是规则（技术规则+ 制度规则）之争；衡量其成功与否的标准，则是能否真正有益于“实现好的社会”。

参考资料

姚余栋，杨涛.共享金融：金融新业态 [M] .中信出版社，2016

罗伯特·席勒.金融与好的社会 [M] .中信出版社，2012

杨涛.区块链——构建共享共赢式金融发展生态体系 [J] .当代金融家，2016（2）

杨涛.区块链与金融中心化挑战 [J] .当代金融家，2016（4）

杨涛.新技术引领数字货币演变 [N] .人民日报，2016-05-03

中国人民银行支付结算司.2015年支付体系运行总体情况.中国人民银行，2015

美联储.Strategies for Improving the U.S. Payment System，美联储网站

美联储.Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption

[27] 本章由杨涛写作完成。杨涛，研究员，博士生导师。中国社会科学院金融研究所所长助理，中国社科院金融所支付清算研究中心主任、中国区块链研究联盟主任。研究方向：货币与财政政策、金融市场、产业金融、政策性金融、支付清算。

[28] [美]梅兰妮·斯万.区块链：新经济蓝图及导读 [M] .北京：新星出版社，2015.

[29] 王强.银行网点过时了吗 [N] .财新网，2015-03-26.

[30] 上海金融学会票据专业委员会课题组.区块链技术如何运用在票据领域 [N] .上海证券报，2016-04-23.

[31] 蔡钊.区块链技术及其在金融行业的应用初探 [J] .中国金融电脑，2016（2）.

第七章

区块链政策与法规^[32]

一、各国政府的监管态度

（一）对加密货币的态度

比特币作为区块链技术运用的典型代表，已存在了数年之久，比特币的广泛使用与随之而来产生的影响力已经让各国的立法者无法忽视。各国针对比特币制定了相应的监管政策。尽管像比特币这样的加密货币因为“货币属性”而具有一定的特殊性，但仍可以帮助我们来推测各国政府对区块链技术可能采取的态度。

1. 美国

美国意识到数字货币如比特币可用来支付商品、服务或持有用作投资。2014年3月，美国关于数字货币的指引，认为数字货币不是货币，而是一种商品，对比特币交易应当征税。^[33]这意味着在美国对于诸如比特币、莱特币或其他加密货币的使用将会支付更高昂的成本。

2014年6月，美国加利福尼亚州州长签署了一项编号为AB129的法律，保障加州比特币以及其他数字货币交易的合法化。该法律规定，在确认不违法的前提下，法案将保障包括数字货币的替代货币在购买商品、服务以及货币传播中的使用。美国纽约州在2014年7月公布了监管比特币和其他数字货币的提案。提案提出要在纽约州开展经营活动，从事数字货币的买卖、存储或者兑换的公司必须要申请许可证。依照提

案，比特币公司不仅仅需要追踪其客户的物理地址，还需要追踪利用比特币网络向其客户转账的人的物理地址。这会降低比特币的基本价值。最大的比特币交易平台之一的Coinbase于2015年1月在美国得到了包括纽约州、加州在内的25个州的认可，未来有望获得更多州政府的认可。

美国商品期货交易委员会（U.S. Commodity Futures Trading Commission）在2015年9月正式将比特币和其他数字货币定义为商品。该委员会将监管比特币相关的交易活动。在美国如果一家企业想要经营一个比特币衍生品或期货的交易平台，将需要申请成为掉期合约执行机构或指定合同市场。

2. 欧盟

德国联邦金融监管局在2011年11月制定了一份“金融工具”备忘录，赋予“比特币”与外汇同等的地位，并规定比特币为一种“记账单位”（Unit of Account），而非法定支付手段。2013年8月，德国财政部宣布，德国或将认可比特币是一种记账单位，但不具备充当法定支付手段的功能。比特币的持有者将可以使用比特币缴纳税金或用作其他用途，德国也将成为全球首个认可比特币的国家。

2015年的“巴黎暴恐事件”发生后，匿名者黑客组织附属组织“幽灵安全”（GhostSec）称，他们相信比特币是极端组织“伊斯兰国”加密货币的首要形式，并且已经在“深网（Deep Web）”上定位到几个“伊斯兰国”用来接受捐赠的网站。为应对恐怖主义使用加密货币所带来的威胁，欧盟委员会计划强化对“非银行支付方式”的控制，如电子支付、匿名支付、数字货币支付以及黄金和其他贵金属的转移。法国的中央银行法兰西银行在2016年发布了一份题为《数字时代的金融稳定性》的新报告，在报告中提到法兰西银行正在考虑跟随区块链技术的发展计划，既包括区块链可能的应用，还包括区块链存在的问题，特别是安全性。

2015年10月，英国财政部的经济秘书哈里特·鲍德温在一次演讲上

表示，英国正致力于将数字货币交易所引入监管体系，并努力为加密货币企业创立合适的制度以吸引海外投资者到英国投资，且英国财政部先后设立了1000万英镑的加密货币研究资金。

2015年10月，为了澄清了欧盟内部对于比特币属性的争议，欧盟法院（Court of Justice of the European Union）做出裁决，认为比特币应该被视为一种支付手段，根据欧盟的相关法律，这种交易应免征增值税。该裁决免除了比特币的税收威胁，否则将增加购买或使用比特币等数字货币的成本。该裁决向比特币合法化迈出坚实一步，加快了比特币在欧盟的市场的进一步发展。这项新规源于2014年6月发生在瑞典的一场争论。当时，瑞典税务局与比特币论坛运营人丹尼尔·海德奎斯特（Daniel Hedqvist）就比特币交易是否需要缴税这一问题展开了争论。

3.中国

2013年12月，为了应对比特币交易在市场上的日益流行，中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会以及中国保险监督管理委员会五个行政部门联合发布了《关于防范比特币风险的通知》。在通知中明确：“虽然比特币被称为‘货币’，但由于其不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义的货币。从性质上看，比特币应当是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。”消息发布后，在全球范围内比特币的价格急转直下，当时全球最大比特币交易市场Mt.Gox在一天之内的跌幅就达到了29.44%。该

《通知》同时要求“各金融机构和支付机构不得以比特币为产品或服务定价，不得买卖或作为中央对手买卖比特币，不得承保与比特币相关的保险业务或将比特币纳入保险责任范围，不得直接或间接为客户提供其他与比特币相关的服务”。通知的出台基本划定了金融与比特币之间的红线。自此以后，中国监管层面后续再没有就比特币出台其他相关规定，但银行根据上级部门的约谈或电话的要求开始对比特币交易关闭充

值接口，看似给以比特币为代表的加密货币判了“无期徒刑”。

但在2016年1月20日举行的央行数字货币研讨会上，传递了一个明确信号：央行将争取早日推出数字货币，并早在2014年就成立了专门的研究团队。只是加密的算法、防伪技术因为涉及国家金融安全，肯定会不同于比特币。至于央行后续是否会选择基于区块链技术的数字货币，需要看进一步的研究结果，但数字货币的发展已势不可当。

（二）对区块链的态度

区块链技术方兴未艾，目前各个领域的运用还算不上随处可见，更多的是开展可行性研究。但区块链技术所具有的潜力依然获得了政府，尤其是金融监管机构的高度重视，考虑将区块链技术投入政府服务中去。

2015年5月，洪都拉斯政府与美国区块链企业公证通（Factom）合作，以建立一套基于区块链技术的土地登记系统。^[34]不过该项目在实施过程中遭遇了挫折，据公证通发布的新的进展公告，称其先前宣布的概念证明项目已经“停滞”。

据韩国央行在2016年1月发布的一份最新研究报告显示，韩国央行正在密切关注区块链技术的发展，甚至在自己研究区块链技术。这份报告由韩国央行的支付系统研究小组撰写，介绍了数字货币和分布式总账技术，并对该技术在未来的发展状况做出了预测。报告认为数字货币还不太可能成为主流应用，因为价格波动过大、技术操作复杂、面临被黑客攻击以及终端用户丢失私钥的风险。^[35]突尼斯政府则计划通过Monetas所提供的区块链技术发行本国货币。Monetas在突尼斯首次实现了完整的数字支付生态系统中的应用。随着Monetas驱动的法国邮政突尼斯安卓应用程序的推出，突尼斯人将可以使用他们的智能手机，实现瞬间移动汇款、在线支付商品和服务、支付工资和账单、管理政府官方

身份证明文件。2016年2月，中国人民银行行长周小川接受媒体采访时，也表示央行在发行数字货币时会考虑使用区块链技术，对区块链技术的优缺点进行进一步的研究。

英国政府科学办公室在2016年1月发布了名为《分布式账本技术：超越区块链》的报告，报告中强调分布式账本技术可以实现完全透明的信息更新与共享，减少欺诈、腐败，降低错误率和用纸成本，提高行政效率，并重新定义政府与公民在数据共享、透明性和信任方面的关系。2016年4月，英国内阁办公室部长马特·汉考克表示，区块链技术能为政府提供一个以公开可验证的方式来监控资金的移动，可以利用区块链的透明性对资金支付到研究中心发挥更好的控制，以帮助学生组织或个人。英国政府目前正在探索使用区块链技术提高纳税人税款的分配效率，例如补助金。英国政府正在查看如何使用区块链技术来管理和跟踪公共资金的分配，例如补助金和学生贷款，马特·汉考克认为区块链技术可能会“推动产生一种新的信任文化”。

澳大利亚标准机构标准澳大利亚（Standards Australia）在2016年4月已经要求国际标准化组织（ISO）为区块链技术设定全球标准。Standards Australia的行政长官艾德里安·奥康奈尔表示：“在全球不同区块链交易商之间实现区块链的互操作性是释放区块链潜力的关键。这就需要有全球标准来释放区块链潜力，而最好的方式就是通过ISO来实现。”

二、区块链资产的合法性问题

在互联网领域，各种新技术高速发展、层出不穷，各种新型权利也不断涌现。法律法规对新型权利的认可难免滞后，很多新型权利无法及时得到法律法规的认可，因此应谨慎判断互联网领域的合法性。

区块链技术正是互联网领域最新的发展成果之一，讨论区块链资产的合法性问题，应综合考虑区块链资产是否具有强大公众需求和商业应用前景，是否损害公众利益，是否影响网络安全。并需要从现行的法律制度、司法实践或行政机关的态度中查找区块链资产的法律依据。

区块链技术拥有巨大的商业潜力，各种基于区块链技术的产品不断涌现。包括中国在内的各国政府也都对区块链技术持开放态度。对于区块链资产，只要不违反法律法规，不损害社会公共利益，其合法性就可以得到保障。

（一）法律

《宪法》是国家的根本大法，也是拥有最高的效力的法律。《宪法》第十三条对财产保护进行了规定：“公民的合法的私有财产不受侵犯。国家依照法律规定保护公民的私有财产权和继承权……”根据《宪法》的规定，区块链资产只要是合法取得的，就应是受到法律保护的财产，并且可以享有私有财产权和继承权。

在我国的民法体系中也有着类似的规定，《民法通则》第七十二条规定：“财产所有权的取得，不得违反法律规定。”同时，《民法通则》对公民个人财产的类型进行了开放式的列举，以备新的财产类型出现，《民法通则》第七十五条第一款规定：“公民的个人财产，包括公民的合法收入、房屋、储蓄、生活用品、文物、图书资料、林木、牲畜和法律允许公民所有的生产资料以及其他合法财产。”该条文列明了财产的范围，并且明确了取得财产权的条件。尽管在《民法通则》中没有明确规定区块链资产或者网络资产，但区块链资产毫无疑问属于“其他合法财产”的范畴。只要是通过合法方式取得的区块链技术资产，如通过交易、继承、生产的途径取得区块链资产的所有权，就没有理由不受到法律的保护。

对于针对区块链资产的刑事犯罪行为，可以依据《刑法》进行打

击。在《刑法》中所列明的财产犯罪中，相关罪名都明确规定了犯罪行为对象是财物，也就是以财物为目标的犯罪。区块链资产可以作为一种新型的财产，受到刑法的保护。对针对区块链资产的犯罪，有关部门有责任维护公民对区块链资产所享有的合法权益。

简而言之，尽管在现行法律中没有对区块链资产是否合法进行明确的规定，未来的立法（如《民法典》的制定）过程中也不会有专门提到区块链类型的资产，但我国在立法上对财产的范围采取了开放的态度，区块链资产并没有被排除在合法财产的范围之外，因此受到我国法律的保护。

（二）监管态度

尽管我国的行政机关对比特币的使用持谨慎态度，但对区块链资产却持开放态度，在五部委发布的《关于防范比特币风险的通知》中，在否定比特币的货币属性的同时，认同了比特币作为一种可以交易的虚拟商品的存在。在2014年的博鳌亚洲论坛上，中国人民银行行长周小川也表示：“……比特币像是一种能够交易的资产，不太像支付货币，……

（比特币）作为资产进行为交易，并不是支付性的货币，所以应该说不属于我们有没有一个什么取缔的问题。”^[36]可见，即使对于比特币而言，在有关部门的文件以及金融领导表态中也未曾否认比特币的合法性，只是对于比特币作为货币可能扰乱金融秩序保持了高度的警惕。

因此，对于区块链资产的商品属性，在不会扰乱金融秩序或违反其他法律法规（如危害网络安全或其他财产安全）的情况下，有关部门也没有否定其存在的必要和理由。在“万众创新，大众创业”的大背景下，有理由相信有关部门对区块链这样的新技术本身更多的会持中立，甚至是持欢迎的态度。

（三）司法案例

在立法尚未完善时，法院对新型技术所涉案件的裁判结果是判断新型技术是否具有合法性的风向标。如果法院不支持保护某新型财产的权利，那么就很难认为该财产具有合法性，反之亦然。近年来，各种新型资产不断涌现，其中最为典型的的就是虚拟财产的广泛使用，而法院对于虚拟财产的态度或可以为日后对待区块链技术的纠纷所借鉴。

在李宏晨诉北京北极冰科技发展有限公司娱乐服务合同纠纷案^[37]中（该案件是我国第一例关于网络游戏虚拟财产的案件，也被称为“红月案”），法院在法律法规没有明确规定虚拟财产属性的情况下，对网络游戏道具进行了处理。在红月案中，一个重要的争议焦点是案件所涉的虚拟装备的价值及李宏晨损失的证据证明情况，法院就此焦点认为“玩家参与游戏需支付费用，可获得游戏时间和装备的游戏卡均须以货币购买，这些事实均反映出作为游戏主要产品之一的虚拟装备具有价值含量。”所以法院最终支持了李宏晨要求北极冰公司赔偿虚拟道具的诉讼请求。在“红月案”后，有关虚拟财产的案件有增无减，涉及盗窃、权属、继承等问题的纠纷层出不穷，法院也都一一进行了裁判。

在法律对虚拟财产没有明确进行规定的情况下，法院依然根据法律原则及法学理论承认了用户对网络游戏中虚拟的道具所享有的权利，并且判决游戏运营公司进行赔偿。可见，法院对于法律尚未明确规定的新型网络财产不会拒绝承认其合法性，更不会拒绝裁判。因此，法院在审理基于区块链技术资产的有关案件时，因为区块链资产本身具有使用价值与交易价值，所以可以得到法律的保护。

三、区块链与法律的重构

（一）代码即法律

长期以来，代码都是规制网络空间中行为的一股重要力量。劳伦斯

·莱斯格（Lessig）教授对此进行了经典论述：代码与法律、市场、准则共同对网络空间中的各种行为进行调整，基于代码的软件或与协议会决定人们利用互联网的方式。[\[38\]](#)

现行的与互联网相关的法律法规需要以如TCP/IP协议、防火墙技术、域名解析技术、超链接技术、数字签名技术等网络协议为基础的，更高级一些如微信平台、微博平台、淘宝平台的技术也是各种网络规范的基础。与TCP/IP协议、微信平台或其他网络上的代码一样，区块链技术同样会对各种网络行为产生深远的影响，并且直接影响到相关的法律关系、涉及的法律主体，以及崭新的法律客体，从而促使现行的互联网法律制度相应地进行调整。即使目前在行业中区块链应用程序非常的少，但仍有许多人都相信区块链技术具有巨大的发展前景。目前，越来越多国家正在达成一个共识——在政府出台有关规定之前，应该对区块链的好处和成本进行精确的分析。

一般认为，区块链技术具有以下技术特征：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）、时间戳（Time stamp）、非对称加密（Asymmetric Cryptography）等。正是这些技术特征的存在，使区块链技术的应用特点十分显著：去中心化的分布式结构应用于现实中可节省大量的中介成本；不可篡改的时间戳可解决数据追踪与信息防伪问题；安全的信任机制可解决物联网技术的核心缺陷。[\[39\]](#)也正是因为区块链的优点，让基于区块链系统的网络资产与以往任何的网络的财产（如域名、账号、网络游戏道具等）都不相同，主要表现在：

- ①区块链资产并不存在一个中央节点；
- ②每一个节点都会存储全部网络的系统信息；
- ③在区块链系统中资产的变动可以被跟踪；

④区块链系统的资产具有更高的安全性。

最近麦肯锡公司发表了一份针对“区块链技术”的研究报告，该报告预测区块链技术将极大地重塑资本市场、影响商业模式并节约成本。根据区块链技术所具有的特点，《经济学人》将区块链技术描述为“一台创造信任的机器。”区块链技术改变了关于互联网上一切与信任有关的经济模式，让可信第三方变得不再必要。在传统网络交易的模式里，需要可信第三方提供担保，可信第三方可以至少具有以下三个方面的功能：

①证明交易的物品实际存在；

②避免多重交易；

③预防交易纠纷，记录交易历史。

传统互联网上信任的建立有赖于可信第三方的存在，比如在淘宝网上购买商品，需要使用支付宝作为可信的第三方负责担保并中转资金，在买家收到货物后再将款项从支付宝转移到卖家。尽管被称为“可信”第三方，但是作为交易的局外人，始终要面临谁来监督可信第三方的问题。而区块链技术的意义在于区块链资产的网络交易无须支付宝这样的第三方提供信用保证，就可以提供可被信任的交易模式，不会涉及谁来监督可信第三方这样的问题。中国信息化百人会成员、中国农业银行副行长林晓轩认为：“区块链技术从根本上改变了中心化的信用创建方式，它运用一套基于共识的数学算法，在机器之间建立信任网络，从而通过技术背书而非中心化信用机构来建立信用。通过这种机制，参与方不必知道交易对手是谁，更不需要借助第三方机构来进行交易背书或者担保验证，而只需要信任共同的算法就可以建立互信，通过算法为参与者创造信用、产生信任和达成共识。”^[40]通过区块链技术，交易的合同可以直接嵌入到被交易过程中，在一定条件下合同条款被触发而自动履行。进一步来说，如果区块链技术与物联网技术结合，甚至可以让这

些变革延伸到线下的现实生活中。

借助区块链技术所特有的信任机制，可以让交易的过程变得更加简洁。比如唯链就致力于提供一个基于区块链技术的真假校验云平台，贯彻区块链即服务（BaaS: Blockchain as a Service）的理念，把区块链当作一个基础设施，并在上面搭建各种满足普通用户需求的应用。随着对区块链技术应用水平的不断提高，会有越来越多的领域受益于此。

（二）知识产权

1. 知识产权登记

近年来知识产权（Intellectual Property, IP）的概念日益得到重视，各行业的知识产权意识也显著增强。知识产权包括版权（著作权）、商标、专利、商业秘密等。

在这些不同类型的知识产权中，商标与专利的获得均需要向有关负责机关进行申请登记后方可获得权利。版权虽然在作品创作完成时就可以获得，但为了证明版权的获得时间，也可以向有关机关进行登记以获取著作权登记证明。因此，知识产权的效力严重依赖于登记机关对于知识产权信息的记录情况。而一旦知识产权登记机关的登记系统出现故障，如不能正常进行登记或登记信息有误，将会给知识产权权利归属的判断带来不便。国家商标局在2014年年中就曾因为系统升级中出现较大技术故障，导致商标审查工作停滞近四个月，致使216万商标申请“暂时性积压”。^[41]无独有偶，美国专利与商标局（United States Patent and Trademark Office）在2015年12月也出现技术故障，导致专利与商标的申请、查询、付费等功能无法正常使用。^[42]类似的故障不仅会造成知识产权申请的积压，更会影响到知识产权的日常运作与管理，导致整个知识产权体系无法正常运行。这样的故障哪怕只发生一天，也会给知识产权行业造成不小的影响。因此，一套安全、可靠的知识产权登记系统是

必不可少的。

现行知识产权体系严重依赖于中央登记制度。而在信息登记方面，区块链技术具有先天的优势，时间戳功能可以提供可信的知识产权登记记录，证明知识产权的登记时间。另外，区块链技术所具有的分布式存储结构能够有效避免因为中央节点系统故障而导致整个登记系统瘫痪的情况发生。因此，对知识产权的登记制度来说，区块链技术有能力提供更加可靠的技术保障。

作为一种所有权账本，基于区块链的注册与传统的数据登记相比，有着独一无二的优势：区块链数据库的去中心化且加密安全性质使它不太可能会遭受灾难性损失或失败，又或者遭受黑客攻击。而且，区块链注册过程几乎是瞬时的，并且可以降低注册成本。除此以外，作品的后续交易也会被实时记录，并且在交易网上可以被追踪到。同时，鉴于区块链的公开性，区块链注册可以使更多的人知道作者对作品拥有所有权，有利于宣示权利归属。但除非官方登记机构使用区块链技术进行登记，其他非官方的登记均需要解决证明效力的问题，即在出现争议时有效证明知识产权的登记时间。

2.作品发行

作品的发行、传播是一项重要的知识产权权利，而在作品发布以后的传播过程中，版权人往往是对整个过程缺乏控制的。尤其是在互联网时代，作品的复制与传播几乎没有成本，也导致了盗版的盛行，未经授权使用他人的文字或美术作品屡见不鲜，这让许多产业深受其害，唱片产业甚至一蹶不振，游戏、电影产业投入了大量资源以求遏制盗版，但效果始终有限。而将区块链技术的引入作品的发行有望改变盗版泛滥的窘况。

区块链技术也有望对网络上普遍存在的版权侵权行为进行遏制。传统上，因为网络上的各类知识产权因为计算机网络可以实现对信息的无

损复制与低成本传播，导致权利人难以对版权进行有效控制，像盗版、“私服”“外挂”这样的侵权屡见不鲜。利用区块链技术，有望让网络上各类作品本身成为可信登记的证明。版权人借助区块链技术有能力控制、追踪网络上自己的各类知识产权的实时情况，避免像在传统网络环境下一样，作品一经发布就失去控制。作品在区块链系统下进行发布时就可以对使用作品的条件进行约定、限制，以加强权利人对自已的知识产权的掌控力度，形成一种崭新的商业模式。

以软件为例，软件的著作权登记证书记载了软件的作者、创作时间、权利归属等事项。如果软件基于区块链技术来进行发行，在软件的每份拷贝中都记载了软件的基本信息，如权利人的信息、使用软件的范围、使用期限，并且通过区块链技术可以轻易识别未经授权的拷贝，并拒绝盗版拷贝的使用，以给予版权人对软件作品更强大的控制力度。因此，区块链技术可能会成为更加有效的软件数字版权管理（DRM）技术，通过基于区块链技术的播放器、浏览器、阅读器或其他软件，影音、美术、文字等类型作品的网络传播都可以加强对作者权利的控制，更好地维护作者的权益。

正是因为区块链技术对于知识产权作品发行的天然优势，基于区块链的知识产权众筹模式也被提出。而位于德国柏林的Ascribe公司就通过使用基于区块链技术的记账系统，让作者可以固定作品的权利属性，安全进行分享并追踪作品的传播。并且可以通过区块链系统对作品的真实性进行真名，在发行时也可以限制发行的数量。音乐人伊门·哈普（Imogen Heap）也提出希望能够建立一套基于区块链技术的简单直接的交易模式，音乐人的作品直接面向听众销售。据使用过该平台的用户介绍，使用该平台的流程是：①登录歌曲“发行”页面；②启动Prototype（使用“数据区块链”所需的前端框架）；③点击歌曲的“下载”；④建立以太账本钱包；⑤用比特币给第④步建立的钱包充值；⑥钱包到账的时候，正式的下链接出现。

利用区块链技术来进行作品发行，有利于让版权人获得对作品传播过程更完整的控制，这将导致利益的天平可能会向版权人一方倾斜。

（三）登记制度

登记制度在法律领域内被广泛运用，除了知识产权登记制度以外，还有不动产登记、机动车登记、企业工商登记、部分财物的交易登记、股权登记、诉讼立案登记等。在这些登记制度中，有些不经登记会导致法律行为无效，这通常是一些特殊权利变更的登记，比如《专利法》规定：转让专利权的，当事人应当订立书面合同，并向国务院专利行政部门登记，并由国务院专利行政部门予以公告，专利权的转让从登记之日起生效。还有一些是不经登记就无法继续推进流程，比如进行立案登记是法院受理、审理与执行案件的前提条件。

传统上对于权利的记录依赖于纸质凭证，近些年随着电子政务的推进，开始越来越多地使用中央数据库对权利凭证进行登记、管理。以股权为例，《公司法》第三十二条第二款、第三款规定：“记载于股东名册的股东，可以依股东名册主张行使股东权利。公司应当将股东的姓名或者名称向公司登记机关登记；登记事项发生变更的，应当办理变更登记。未经登记或者变更登记的，不得对抗第三人。”股权虽然不是强制要求登记，但如果不在管理部门进行登记，会面对无法对抗第三人的后果。区块链技术无疑可以帮助有关管理部门进行登记。在权利变更的过程中，登记是权利变更流程的一部分，但变更程序是复杂、缓慢且昂贵的，由于变更登记往往会涉及大量的资金，每个人都需要进行足够的尽职调查。因此，区块链成为保证这些调查的候选者。以不动产交易为例，买家和贷款人都需要对不动产的价值进行评估，买家和贷款人要求土地登记，对周边环境、房屋内的户口情况、学区等问题进行调查，有时还需要了解借款人信用检查，这无一不是交易中可能的障碍，而所有这些调查依赖于开放和信任的数据源。国内创业团队小蚁

（AntShares）做的就是将实体世界的资产和权益进行数字化，用区块链

技术解决资产的登记发行、转让交易、清算交割等业务。

目前，Bitland(宝龙达)提出了一种新的区块链技术项目，目标是提供允许个人和团体在Bitland区块链上进行土地调查和土地所有权记录的服务，提供永久性的、可审计的记录，并作为一个联络机构帮助解决纠纷。该项目旨在消除腐败，并且声称能够释放价值数万亿美元的基础设施建设产业。项目首先在加纳最大城市之一库马西（200万人口）的28个社区进行试点，长远目标是将这个服务推广到整个非洲大陆。

（四）网络财产

网络早已成为人们社会生活中不可或缺的一部分，越来越多的财产也从线下转移到了线上。我们的电子邮箱、域名、各种网络服务的账号等具有经济性的财产都成为我们日常生活中不可抛弃的部分。因为网络上的各种安全风险，导致这些财产不时面临黑客入侵窃取、篡改、删除数据的隐患。而关于这些财产的归属权问题，尽管普通用户可能未曾留意过，但绝大多数的网络财产的所有权都归于网络服务的提供商所有，用户只是享有使用权。网络服务提供商与用户之间通过用户协议约定了虚拟财产的所有权归属。

传统上，因为网络财产大多存储于网络服务提供商的服务器中，网络服务提供方可以随时进行修改、删除等操作，因此提供网络服务的一方对网络财产具有绝对的掌控，用户的处置权利有限。而基于区块链技术的网络财产，尽管可以通过应用软件设置各种权限，但还是会被储存在每一个节点中，而这样的存储方式无疑会削弱网络服务提供方对财产的掌控力度，用户对网络财产的掌控会在一定程度上得到加强。而这样的改变会影响到网络财产的归属等一系列问题，网络财产归属的平衡可能会被打破，用户会对网络财产享有更多的权利。

借助区块链技术，可以开发出基于区块链技术的网络财产管理系统。网络服务的提供商通过区块链账号管理系统有能力加强对各类型财

产的控制，降低中央服务器被攻击、拖库而导致的服务瘫痪、隐私泄露的风险。对于用户来说，区块链技术有能力带来更高的安全性，以有效降低网络财产所面临的安全风险，并且可以提供一种更加便利的使用权证明，方便各方确定网络财产的权利与义务，避免因服务协议或内容的变更导致的用户权益受损。

（五）从电子合同到智能合同

随着互联网经济的日益活跃，电子合同因为具有便捷、高效的特点开始被广泛利用，如用户在注册网站时所点击同意的“用户协议”、电子商务平台为了交易方便而与供货商利用网络所签订的“供货合同”、互联网金融的有关交易等，都依赖于有效力的电子合同。电子合同甚至可以说是大多数互联网交易活动的法律基础。国务院在2015年5月制定的

《关于大力发展电子商务加快培育经济新动力的意见》第一次明确提出了“建立电子合同等电子交易凭证的规范管理机制，确保网络交易各方的合法权益”。电子合同因为完全是在网上进行操作，所以保证电子合同的真实性是重中之重，目前主要是以电子签名的形式进行保证。在常规集中的数据库，这些交易是由一个单一可信权威管理机构创建的。相比之下，由区块链驱动的共享数据库，交易可以由任何一个区块链的用户创建。而且，由于这些用户不完全信任对方，数据库必须含有限制进行交易的规则。例如，在一个点对点网络的财务分类账，每一笔交易必须保持资金的总量不变；否则，用户可以随意给自己取尽可能多的钱，因为他们都很喜欢。

甲骨文公司洞察与客户战略部门副主管萨波拉曼尼亚·艾耶

（Subramanian Iyer）认为，区块链可以容纳大量的数据，包括完整的合同。智能合同会消除如法律公司这样中间人的存在，当特定的一些条件获得满足的时候，支付将会自动进行。就其本质而言，智能合约以电子的方式很容易执行，它通过脱离单一机构的掌控创建了一种强大的第三方机构。借助区块链技术，电子合同可以具备相较于传统电子签名更高

的安全性。更重要的是区块链技术可以让合同文本与合同内容紧密地结合在一起，像网络财产、网络版权作品都可以将合同文本嵌入其中，让合同内容根据约定的情况自主去履行权利与义务。例如在线影音作品的租赁。如果借助于区块链技术，在影视作品的拷贝中嵌入合同的内容，在视频中嵌入著作权人的信息以及授权用户观看的时间、范围，以减少抄袭或其他侵权行为的可能，甚至可以设置按照观看的进度来进行自动付费。因此，简而言之，智能合同其实是一段被存储在一个区块链上的代码，由区块链交易触发。[\[43\]](#)

而随着网络环境的变化，面对可以自动履行的合同，传统合同法中的部分规定可能将不再适用。在中国现行的《合同法》中，第四章专门规定了“合同的履行”，而随着基于区块链技术的智能合同广泛运用，合同履行或许会与合同文本的制定融为一体。在智能合同时代，如果智能合同在履行时出现瑕疵，可能并非是因为合同履行方没有去履行合同，而是智能合同在研发时存在隐患，导致具有履行合同义务的一方无法履行。这时，可能就会需要智能合同的提供方或开发方就合同不能履行承担相应的法律责任。简而言之，智能合同的运用会让合同的权利、义务重新划分，以适应智能合同所带来的变革，而这需要对现行的《合同法》根据区块链技术的特点进行修订。

信达证券首席区块链专家曹寅认为：“在区块链时代，传统的社会契约形式，将被对于基于区块链的智能合同的运用前景。”汤森路透的副总裁兼产品管理负责人斯科特·曼纽尔表示，他们的许多法律客户对智能合约的潜力，智能合约能够做些什么，以及它们在区块链世界中允许什么很有兴趣。区块链以点对点信任直接传递和强制信任化的功能，实现了生产关系的解构，其解构原理非常类似“物理第一性原理”对于宏观物理现象的解构，任何尺度的宏观物理现象，不管是山崩地裂，还是日月运行，都可以用最基本的质子和电子间的关系来解释。在区块链时代，任何经济行为，不管是股票发行还是破产清算；任何组织形式，不管是创业合伙还是跨国企业，都将被区块链解构，解构为最基本的人和

人之间的经济行为。

以太坊（Ethereum）项目正是一个提供智能合同的去中心化平台。平台上的应用在运行时可以被设计，允许用户编写复杂的智能合同，担保和交易任何事物：投票、域名、金融交易所、众筹、公司管理、合同、知识产权等。比如在接收货物时能创建电子发票，或者在利润达到一定金额时自动向股票持有者发送分红。还可以设置以太坊区块链内置的汽车钥匙，遵循相应规则进行出售或出租，产生新型的P2P汽车租赁或共享。2016年4月，区块链技术专业公司Gem(宝石)官方正式宣布推出Gem Health（宝石健康）项目，以推动医疗领域的新兴技术的合作和发展。Gem在公告中表示，飞利浦公司将会成为他们的第一个合作伙伴，飞利浦将会帮助Gem以构建一种能够用来开发企业级医疗应用程序的私有以太坊区块链。

（六）物联网与区块链

物联网是一种基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。统计显示，在2015年通过无线网络进行连接的物联网设备就已经达到134亿台，预计到2020年将会有超过280亿台物联网设备。万物互联的景象似乎已经近在咫尺。

区块链技术有望协助解决物联网发展所面临的一些技术性问题，比如成本、诚信以及防护。对物联网设备进行中心化的追踪和管理不仅在技术上难以实现，这样的尝试也不明智，而在去中心化物联网中，区块链可以被用于促进交易的处理和交互设备间的协调，每一个物联网设备都会管理自己在交互作用中的角色、行为和规则。与物联网设备结合，基于区块链技术的智能合同可以将网络上所能利用到各种便利服务扩展到实体物中。区块链技术可以在无须信任单个节点的同时创建整个网络的信任共识，从而很好地解决物联网的一些核心缺陷，让物与物之间不

仅连接起来，而且能够自发地活动起来，互相进行认证，让我们更好地利用物联网所带来的便利。[\[44\]](#)

在纽约布鲁克林区，区块链正在使新型的微智能电网，最终能够允许点对点技术，超本地绿色电网从传统电网中独立运行。分布式能源将彻底改变能源市场如何运作。埃森哲咨询公司也正在验证使用区块链技术打击假冒药品的项目的可能性。而创业公司HelloSent认为智能合同和物联网设备可以用于监测红酒的交付，HelloSent将基于区块链技术传感器用于运输中连续测量红酒的温度和湿度，如果任意一项低于智能合约中记录的约定水平，那么购买订单将会自动取消，以此来保证所销售葡萄酒的品质。这种应用模式完全可以用于疫苗、食品、危险品的运输存储过程中，区块链技术有助于监控这类需要冷链或专门保存条件的运输过程。

除此以外，区块链技术还可以帮助物联网设备的所有人实时跟踪自己财产的真实状态，包括财产的地理位置、完好程度、使用人资质、过往交易记录、担保情况等信息。这可以让实体物的交易、使用可以像在网络上一样得到有效监控。线下的房产交易租赁、汽车的销售租赁、物联网所收集个人信息的安全，都有望借助于物联网技术与区块链技术得到更好的解决方案，以减少各类因为登记信息被篡改或伪造产权证明所产生的争端。另外，区块链技术也能够让对于财产的执法行为变得更为容易，有效避免为了躲避对财产执行而对财产进行的转移。像空中住宿（Airbnb）这样的房屋短租公司也开始关注区块链技术，在2016年雇佣大量ChangeTip员工，以对区块链技术在短租领域的商业运用进行研发。Airbnb的用户能找到心仪的短期住所，一个重要的原因是Airbnb拥有一个相对完整的评分和评论数据库，以存储房屋主人和房客的评价交易信息。而像记账本一般的“数据区块链”能够储存几乎所有交易、评分和评论明细，从而将数据变得更加可读。另外，以“区块链”的方式安全、谨慎地将数据“出口”到其他平台，或者共享数据。

但是，在看到区块链技术与物联网结合的潜力的同时，也不应忽视其潜在的法律风险。伴随着物联网数据存储而来的信任问题和身份问题，隐私和个人数据的保密将是物联网市场发展不得不跨越的障碍。换句话说，区块链技术或将成为全球连通数字与物理世界的基础设置，包括可穿戴计算、物联网、传感器、智能手机、笔记本电脑和照相机、智能家居、智能汽车，甚至智能城市可能都会基于区块链技术，区块链上每一个节点都会记录全部数据库的数据，这也会导致用户的隐私问题随之而来，毕竟没有人希望在使用自己财产时处于时刻被他人监视的状态，或者是存在被监控的可能。需要技术开发者在提升区块链与物联网技术用户体验的同时，做好用户隐私的保护工作。

（七）区块链鉴证

1.证据的真实性

无论是解决哪一类型法律纠纷，对证据真实性的确认总是重点。如果无法保证证据的真实性，那么无论证据看上去是多么有说服力都无济于事。但因为现实纠纷的复杂性、专业性与日俱增，法官单纯凭借自己的法律专业知识无从判断一些新型证据的真实性，所以需要借助第三方的专业意见来就证据是否真实进行判断，比如对于借条上签名的真实性需要通过笔迹鉴定来判断，对血缘关系是否真实通过DNA（脱氧核糖核酸）鉴定来判断，对于死者的死因则需要通过法医鉴定来判断，不一而足。

在进入计算机互联网时代后，对电子证据真实性判断的需求更加迫切。在计算机互联网环境下，编辑、复制、传输文件信息不仅简单，成本更是低廉。而随着人们越来越多的商务往来、信息交易、休闲娱乐全部过程都发生在互联网上，在遇到纠纷时或者为了避免纠纷，对电子数据证据真实性的证明需求也越来越高。

但是，电子数据因为具有无形性、隐蔽性强、易被破坏的特点，给

证据真实性的认定带来较多困难。^[45]根据证据规则，无法与原件、原物核对的复印件、复制品是不能单独作为认定的依据，原始文件的证明力也是大于经过复制的文件。因此对电子数据真实性认定是以电子数据证据原件为前提。但计算机等输出的书面材料很难说是原件，且电子数据依附于存储介质而存在。在物理意义上，电子数据是信息附着于存储介质后才生成的，其原件应当指最初生成的及首先固定所在的各种存储介质上的信息，随后无论采取何种方法取得的信息都是该电子数据的复本。因而，何为电子数据的原件在司法认定上难以确定。

传统上，司法实践中对电子数据证据真实性的证明主要通过公证机构进行公证的方法，如证明电子邮件真实性可以通过在公证处登录电子邮箱查看邮件并将整个过程以录像或截屏的方式进行。除了公证以外，还可以使用可信时间戳认证的方式，即通过我国法定时间源和现代密码技术相结合而提供的一种第三方服务，通过可信时间戳证明数据电文（电子文件）产生的时间及内容完整性。无论是通过公证还是时间戳认证，都是借助第三方机构的权威性来证明证据的真实性，而第三方机构的权威性要么是来源于特殊的法律地位，要么是来源于技术上的可靠性。借助第三方机构可以在一定程度上解决电子数据证据真实性的问题，但不可避免地会遇到成本高昂、手续烦琐的问题。而真正造成“麻烦”的是对电子证据真实性的确认无法离开第三方。

2. 区块链技术与证据的真实性

在区块链技术的结构中，每一个节点都记录了数据库的完整历史。区块链上的每一条数据都可以通过“区块链”的结构追本溯源进行验证。^[46]区块链技术也因此被誉为“创造信任的工具”，并且自带有时间戳认证以及加密的功能。在有能力不借助第三方的情况下，提供足以保证证据真实性的证明。以基于区块链技术的比特币为例，根据中本聪的论文《比特币：一种点对点的电子现金系统》中的描述：比特币的“时间戳服务器通过对以区块形式存在的一组数据实施随机散列而加上时间

戳，并将该随机散列进行广播，就像在新闻或世界性新闻组网络的发帖一样”。且“该时间戳能够.....的确存在的，因为只有在该时刻存在才能获取相应的随机数列。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前一个时间戳进行增强，形成一个链条”。因为自带时间认证功能，在网上甚至可以找到用比特币来证明截图的时间的教程，其原理就是基于区块链技术的时间戳不可被篡改性。[\[47\]](#)可见区块链技术在时间认证方面的可靠性。

实际上，已经有区块链技术试图取代公证机构的存在，Stampery公司就试图利用区块链技术所具有的时间戳属性来代替传统公证的效力。将区块链技术引入公证，在无须公证机关介入的情况下，降低用户对证明与时间有关事项的时间成本与经济成本。不过目前Stampery的法律效力还没有得到法院的认可，但创始人对此颇为自信，认为法官会接受Stampery公证的效力，因为Stampery提供的不是观点，而是数学。另外，公证通（Factom）也在利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式。公证通维护了一个永久不可更改的、基于时间戳记录的区块链数据网络。减少进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。公证通的应用远远超出记录保存和资产管理的范畴，它还可被应用在版权、教育和契约法的制定。政府已经找到这项技术的用途，并会继续发掘它的可能。拥有庞大人口的国家可在税收、普查中使用公证通，会大大削减成本。

3.作为证据的区块链技术

区块链作为证据的前提是利用区块链技术进行证明的事项在法庭上站得住脚。从证据的角度需要确保区块链资产在作为证据时的真实性、合法性与关联性，即证据的“三性”。

证据的真实性指服务的内容作为证据事实，需要不以任何人的主观意志为转移，它以真实而非虚无的、客观而非想象的面目出现于客观世

界，且能够为人所认识和理解。证据的合法性是指作为民事案件定案依据的事实材料必须符合法定的存在形式，并且其获得、提供、审查、保全、认证、质证等证据的适用过程和程序也必须是合乎法律规定的。证据的关联性指民事证据必须与案件的待证明的事实之间有内在的联系。与区块链技术本身相关的主要是真实性与合法性的要求，关联性通常需要结合具体案件的情况进行判断。

从真实性的角度来讲，区块链本身就具备了时间戳的属性。即对数据库中的信息形成时间提供可信的证明，并且在整个过程中排除人为干涉的可能，天然具有证明时间的属性。虽然在普通电脑上也可以通过查看文件属性来确认文件的“创建时间”“修改时间”或“访问时间”“作者”“单位”等信息。但是这样的信息并不难被篡改，即没有密码学上的科学保证。在法庭上，只需要演示一下这些文件的属性信息是可以被修改，或是存在被修改的可能性就足以让这些文件的效力大打折扣。与此不同，区块链技术对于时间的证明在现有科技的条件下无法修改，只要在庭审时能够证明基于区块链技术的电子数据证据的效力就不难得到法官的认可。

从合法性的角度来讲，基于区块链技术所提供的内容需要是符合法律规定的。如果利用区块链技术进行窃听、偷拍或胁迫抑或其他违法方式取得，那么该项证据则不具有合法性，不可能在法庭上得到认可。

从举证的角度来说，基于区块链技术所提供的网络服务，无须对提供服务的过程进行逐一的证据保全，只需要在出现纠纷时向法庭展示文件内容，说明系统的原理即可保证证据的真实性。这节省了将大量文件进行公证或时间戳认证所产生经济成本与时间成本，减少了工作流程。区块链系统是一种“天然”的证据保全工具，证据保全伴随着网络服务的过程同步进行，无须专门的流程就可完成证据保全工作，可以为健全网络交易规范、规范网络环境、追究侵权责任方、查处违法违规行为提供

助力，让证据的真实性不再是一个问题，更无须专门为此费心进行证明。不过需要注意的是，为了应对与区块链技术有关的诉讼，需要了解区块链技术原理的律师、技术专家密切配合，清楚、无误地向法庭解释区块链技术，帮助法官了解区块链技术为何能够保证文件的真实性，减少因为解释不清而导致无法认定证据效力的情况。

（八）隐私保护

根据工业和信息化部在2013年制定的《电信和互联网用户个人信息保护规定》，网络个人信息是指用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等数据，并且具备能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。在传统互联网环境下，个人信息主要包括用户上网所产生的信息，如用户在网络上的言论、Cookie中的信息、网络账户的账号及密码、实名登记的身份信息等。在使用互联网时，个人数据不可避免会在网络上传输，而在传输的过程中个人信息就存在被盗用、传播的可能性，这也让每一个网络用户都成为潜在的受害者。个人信息泄露会给信息相关人造成巨大的伤害，使其饱受骚扰之苦。更可怕的是个人信息的泄露往往并不是单一的个案，而是大范围的个人信息泄露，通常会伴随着数以万计的个人信息被窃取、非法贩卖，甚至会利用正规的数据交易机构交易窃取到的数据。

区块链技术所具有的加密性可以为个人信息的保护提供解决方案。区块链技术可以对个人信息进行分布式保存，避免单一服务器所面临的安全风险。

用户还可以借助区块链技术加强对自己个人信息的控制。传统上，用户的个人信息的收集、挖掘、交易等过程被网络服务提供商牢牢控制，用户难以了解到自己的个人数据如何被利用，更难以了解网络服务提供商在利用自己信息时是否存在违规甚至是违法行为，而约束这些网

络服务提供商的，只有与用户之间的用户协议而已。基于区块链技术，可以帮助用户加强对自己个人信息控制力度。区块链所有的交易信息对于用户可以是公开透明的，让用户有办法跟踪自己个人信息的使用情况，有效避免用户在自己的信息被收集后就完全被抛在一边的窘境。

Enigma是麻省理工学院媒体实验室旗下的项目。Enigma是一个基于区块链技术的去中心化的云平台，可以保护隐私安全的去中心化的云平台项目。私人数据在Enigma的存储、分享和分析，完全不会透露给第三方，Enigma取消了对可信任第三方的需要。在Enigma平台上，私人信息可以在不完全泄露给任何一方的情况下进行存储和分析。Enigma平台是基于高度优化的区块链技术的多方安全计算（Secure Multi-party Computation）技术。据Enigma项目创始人光·祖卡德（Guy Zyskind）介绍，整个平台就像是一个“黑箱”，人们可以随意上传任何类型的数据，这些数据在黑箱中被进行处理并返回结果，真实的数据从未被泄露给外部或处理数据的计算机。据《连线》网站的报道[\[48\]](#)，Enigma项目的安全性与节点的数量息息相关，越多的计算机参与其中，用户的数据就越安全，但是处理的速度也会越慢。而当每次有人从Enigma系统中进行计算请求时，需要以比特币支付费用。这笔钱的少部分会支付给区块链系统中一台记录Enigma元数据的计算机。大部分费用会支付给Enigma网络中的节点，以作为存储、处理用户加密数据的奖励。Enigma软件同样可以设置奖励数据的所有者。因此，Enigma的用户，例如广告商可以在不将个人数据破解的情况下向用户支付数据挖掘的费用，让各方都有利可图。

（九）规制区块链

区块链是一项新兴技术，对区块链的规制离不开法律、代码、市场、准则四个方面，区块链技术的应用与发展同样不可能不受这四个方面的影响。

法律规制着使用区块链技术的各种行为。著作权法、侵权责任法、合同法直接对各种利用区块链的侵权行为进行处罚，划定了法律上的红线。比如行政机构对比特币使用的限制就直接影响了比特币的发展。

代码也规制着网络空间的行为。区块链代码本身所具有的特点决定了基于区块链技术各种应用的使用方式。像开放源代码这样的运动可以提高区块链技术的安全性及稳定性，让用户的使用可以更加放心。

市场也是规制区块链技术的重要力量。市场的好恶直接决定了区块链技术的发展前景。另外，如果区块链技术的应用成本过高，那么区块链的应用难免会被局限。也就是说，即使区块链在技术上再领先，如果缺少商业上的成功，那么利益所涉及的各方也不会有太多心思去对区块链进行规制。

准则与法律类似，但在法律尚未健全之时可以起到关键的作用。因此，建立一套区块链技术的应用准则也显得尤为必要。像澳大利亚标准机构(Standards Australia)已经要求国际标准化组织为区块链技术设定全球标准。标准一旦设定，将会对区块链技术的应用起到重要的指引作用，甚至是树立基本的使用规范。

因此，在考虑对区块链进行规制时，需要将目光放的更加长远，思考的角度也需要更加全面，综合考虑法律、代码、市场、准则四个方面，以对区块链技术所面临的潜在问题进行规制。

四、区块链的法律前景

在社会经济发展过程中，技术因素一直都起着重要的作用。社会关系因为技术的发展不断发生着变化，社会关系的变化也让法律的调整成为了必然。与此同时，法律也直接影响着技术的发展，像《促进科技成果转化法》这样的法律法规会直接影响到科技的进步。技术对于法律的

影响永远都是一个复杂的话题，法律制度变迁的背后从来都少不了技术的影子。区块链技术有能力彻底改变互联网上的信任关系，而这对现行互联网法律体系的影响难以估量。区块链技术让网络更像现实，让网络规则更像物理规则。区块链让现实中的物理学定理变成了加密的算法，来保证数据的唯一性。

近年来，无论是在法律圈还是在科技圈讨论“互联网+法律”的人都不在少数，法律人担心互联网会改变现行法律行业的经营方式，而互联网行业从业者们则在试图通过互联网渗透法律这一古老的行业。因此，法律人有必要对互联网技术进行更广泛的了解，互联网行业从业者也有必要了解现行的法律制度。区块链技术为法律制度与互联网的结合与发展提供一种完全不同的可能性，或许未来真的会走上这条路，或许会由于各种原因另辟蹊径。无论是哪种情况，大家都没有理由去忽视区块链技术可能对法律的影响，更不能无视法律对区块链技术的规制。

[32] 本章由史宇航写作完成。史宇航，上海交通大学凯原法学院博士研究生，主要研究领域为知识产权法，对区块链的法律重构有深入的研究。

[33] IRS Virtual Currency, Guidance <http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>。

[34] Honduras to build land title registry using bitcoin technology <http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515>。

[35] <http://bok.or.kr/contents/total/ko/boardView.action?boardBean.brdid=123570&boardBean.menuid=110&boardBean.rnum=2&menuNaviId=2123&boardBean.cPage=1&boardBean.categorycd=0>

[36] 周小川.比特币不像支付货币 谈不上取缔，<http://tech.qq.com/a/20140411/015521.htm>。

[37] 参见李宏晨诉北京北极冰科技发展有限公司娱乐服务合同纠纷案一审：北京市朝阳区人民法院，（2003）朝民初字第17848号；二审：北京市第二中级人民法院，（2004）二中民终字第02877号。

[38] 劳伦斯·莱斯格.代码2.0：网络空间中的法律 [M].北京：清华大学出版社，2009：140。

[39] 区块链：星星之火，可以燎原，<http://www.8btc.com/blockchain-revolution>。

[40] 林晓轩.区块链技术或将根本改变金融机构间的交易规则 [J].中国金融，2016：8。

[41] 216万商标申请“暂时性积压”，<http://www.infzm.com/content/104797/>。

[42] USPTO Systems Status and Availability,
http://www.uspto.gov/blog/ebiz/entry/uspto_power_outage_update。

[43] 智能合约中存在的3种最常见的误解, <http://www.8btc.com/beware-the-impossible-smart-contract>。

[44] 区块链: 星星之火, 可以燎原, <http://www.8btc.com/blockchain-revolution>。

[45] 电子数据真实性如何认定,
<http://www.chinacourt.org/article/detail/2014/07/id/1329854.shtml>。

[46] 区块链: 星星之火, 可以燎原, <http://www.8btc.com/blockchain-revolution>。

[47] 怎样用比特币来证明截图的时间,
<http://btc.cnfol.com/bitebixueyuan/20131220/16523255.shtml>。

[48] MIT's Bitcoin-Inspired 'Enigma' Lets Computers Mine Encrypted Data <http://www.wired.com/2015/06/mits-bitcoin-inspired-enigma-lets-computers-mine-encrypted-data/>。

第八章

区块链经济学的范式革命^[49]

一、自由与演化：发自社区，来自市场

从经济学角度观察区块链的发展，首先会发现它的诞生并非来自政府，也不是出自金融巨头，而是肇始于互联网的社区之中。

区块链来自比特币等数字货币，数字货币的出现是社区形式的，这一点是比特币等数字货币得以在全世界范围发展的重要原因。现在看来，区块链发自社区正是一把“双刃剑”。社区形式的数字货币自从诞生伊始便是市场化的。这句话怎么理解呢？如果我们把整个世界上各种货币之间看成是一个竞争的市场，那么数字货币一方面可以低门槛地参与到这个全球性的市场里，另一方面其一旦跨出这一步，也就等于面临着全球其他所有货币之间的竞争。低门槛表现在数字货币的交易流通相比现有货币市场（外汇市场）更方便。理论上只要世界各地有任何一个民间的多币种数字货币交易所接受了某个数字货币，那么也就等于其已经进入了全球的交易市场之中^[50]。当然进入全球的交易市场并不完全是好事，因为这么做意味着该种数字货币的竞争对象起码也已经是包括比特币在内的其他数百种数字货币，如果自身没有足够的特色和生命力，资本很快就会转移。

读者看到这里可能会提出质疑：数字货币名不正言不顺，所谓的全球交易市场不过是民间的多币种交易所而已，相比外汇市场而言体量微乎其微，凭什么相提并论？

确实，从交易体量上看，即使把现存的所有数字货币以及各种区块链应用代币全都算上去，也就只有比特币能够称得上是“外汇交易品种”。其余各种品类各异千奇百怪的数字货币、区块链应用代币乃至数字资产都和“外汇”一词体现出的世界级别影响力相差甚远，可是，他们却拥有着对于演化而言最重要的条件：自由竞争。

让我们分别从数字货币代表比特币和区块链的发展来观察竞争和演化带来了什么。先看比特币。比特币的发展之路，一是不停地面临着后续其他新生数字货币的竞争和挑战；二是自身的升级和优化方面遇到多种力量的博弈和制衡；三是其在慢慢为世界所接受成为一种新生的外汇品类之时也面临着世界上其他主流货币的竞争和挑战。就第一点来说，其他数字货币往往在基于比特币的基础上提出自身的改良，进而具备更多的特征。这种技术上的改良与挑战对于比特币来说始终是一种压力，也是其不断改进的动力和参考。就第二点来说，从近期比特币的扩容升级问题可以看到，从各种BIP[\[51\]](#)到Core和Classic的派别之分的涌现，正是内生演化的具体表现。就第三点来说，比特币从一个备受争议的虚拟代币，经过数年的发展逐渐从极客的小圈子，从世界范围内的抵触、怀疑到被初步接受、认可的过程，也正是比特币作为一种新生的外汇品种的演化之路。

从以上三点可以看出，比特币内生和外部相关联的演化道路之所以曲折复杂，从表面看得益于开源和去中心化理念积累数十载后于区块链上的突然爆发，而深究其背后的原因便可得知，动力来自于自由竞争和市场。比特币的社区文化可以说便是开源、自由、无国界的互联网文化缩影；比特币内在价值也体现在互联网无国界低租值的货币需要构成上；最后，通过市场的充分竞争，比特币得以在演化的过程中不断历练、充实并完善、提升。演化说里关于生命的诞生有一种观点认为，最初的有机物是从无机物诞生的，而无机物到有机物的跳跃最关键要素之一便是一个良好的“原汤”环境。由此观之，在自由竞争和市场的“原汤”环境下，比特币的出现和成长是一种偶然，也可以说是一种必然。

偶然之处在于比特币竟然活到了现在而没有被无数次危机淹没，必然之处在于就像无机物到有机物的进化一般，货币总会向着数字货币这种更经济的方向进化。

区块链经过近8年的发展，其概念覆盖了账簿、货币、数字资产到智能合约等多个方面。这种不断开花——结果——进化的循环过程正是上述比特币发展路程的全景和衍生。

二、组织与激励：各花入各眼

在区块链发展的过程里，我们经常看到的是其应用如何多姿多彩。有趣的是除了应用和功能以外其发展的土壤——其内部组织架构也在发生着变化。接下来让我们去一探究竟。

①社区型：比特币（Bitcoin），数字货币，2009年至今[\[52\]](#)。

②社区+基金会：以太坊（Ethereum），智能合约，2014年至今。

③基金会+公司型：公证通（Factom），防伪证明，2015年至今。

④公司制：各种联盟链、私链，2015年至今。

从以上四种形式分别看，基于社区形式的组织数量伴随着比特币2014~2015年的价格低谷逐渐减少。但社区形式因其低成本、低门槛，始终维持相当的生命力，并且在2016年通过TheDAO巨额众筹的成功得以另一种形式的发展。作为当前区块链领域的知名项目以太坊，其基金会可谓是毁誉参半。赞同者认为其让以太坊更纯粹和非商业化，质疑者认为其财务管理不善，若非以太（以太坊区块链的代币）暴涨，项目甚至可能中途“夭折”。基金会+公司形式的优点在于运营团队的稳定，但同时也有团队以及资金的归属疑问。

最后一种完全的公司制一般对应的是联盟链和私有链，鲜有公开链的项目。其原因可能在于公开链的共识机制对于独立第三方的经济激励导致其代币（Token）的不可或缺，而代币的扩散与注资往往与挖矿

（PoW）和众筹（PoS）等社区行为相关联。加上开源的默认特点，社区行为以及代币更流行的组织架构是基金会而非公司。公司制的区块链组织稳定，但不够开放。稳定的原因在于其团队激励更多来源于传统的工资以及股权，团队更多体现的是经济人假设的特点——逐利；不够开放其实是指激励的单样性——想象某人为了世界公平，更可能加入某公司制区块链团队还是社区形式？一般理解便是后者。所以在我看来，公司制与社区型的区块链区别更多体现在激励的不同上。

以上四种形式按照其典型案例的出现时间先后排列。可以发现社区型区块链应用出现最早，其后逐渐向公司形式转变。有的读者现在可能在想这样一个问题：上一节不是说到区块链发自我社区来自市场吗，怎么看上去随着时间的推移区块链离社区越来越远了呢？

一般认为社区形式是最为自由也是组织架构最为松散的一种形式；公司形式则是这四种组织形式之中最为规范，目标也最为明确（即盈利）的一种；基金会则介于两者之间。可以这样去理解以上信息：为了更好地适应外部环境，区块链的参与人员由一开始的弱组织形式慢慢向强组织靠拢；同时也越来越偏向于找到一种稳定的、可以长期盈利的模式。从理性人角度出发很容易可以理解这种转变，即任何新技术的诞生可以是偶然的，但其发展和扩张一定满足的是：为自己同时也为社会整体运行带来更低成本、更高效用，实现帕累托优化。

那么是不是说将来的结果就一定是社区形式区块链组织式微，而公司形式的区块链组织越来越多呢？不尽然。帕累托优化的意思是在没有使任何人境况变坏的前提下，使至少一个人变得更好。需要注意，对于每个人来说，更好的含义是不同的。可能出现这种情况：对于甲来说获取更多工资是更好的；而对于乙来说世界公平是更好的。对于甲来说加

入公司制的组织可能是更好的，而对于乙来说加入社区制的组织可能是更好的。由此可以推测，同时存在公司制和社区制的两种组织相比单纯的一种组织，对于甲乙两人来说是一种帕累托优化。

再深究下去，我们会发现这涉及经济学的基础问题：是经济人假设，还是社会人假设？人是经济理性的，还是社会理性的？人是自私的，还是利他的？To be or not to be(是，还是不是)？永恒的问题。[\[53\]](#)

个人认为未来会是越来越偏社区化的，因为我相信随着技术生产力持续不断的指数级别提升，经济激励的效用相对而言会越来越低。

三、纳什均衡：公有链的永动机之谜

经常会看到人们讨论区块链（本节“区块链”等于“区块链公链”）的成本，奇怪的是往往会出现以下两种相反的论述：

①区块链是免费的，低成本的；②区块链很贵很浪费。

到底谁对谁错？都答对了一半。

先看看第一种：“区块链是免费的，低成本的。”这种说法是从用户角度出发而言的。对于用户来说，使用某个区块链应用（例如比特币）进行转账的时候，并不需要考虑比特币的运营和维护费用。用户根据比特币协议理论上只需要付出极少部分的转账手续费即可实现付款。从这个角度来看此论述正确。

再看看第二种：“区块链很贵很浪费。”这种说法是从区块链的设计者或是投资者角度出发的。对于设计者而言心里很清楚“天下没有免费的午餐”这一道理。区块链的设计里不论是PoW（Proof of Work，工作量证明机制）还是PoS（Proof of Stake，股权证明机制），都需要有对

应的资源付出以换取整个系统的共识和平稳运行。在PoW里，资源是矿工挖矿的工作量；在PoS里，资源是购买股权付出的金钱。

图8-1 是比特币PoW机制下的区块链运作机制。作为分布式账簿来说，左边条线是系统运维得以实现的基础，即分布式账簿通过挖矿机制激励矿工维护系统运行。右边条线是系统得以不断扩大的条件，即分布式账簿确实满足了需要进行价值交换用户的需要，在某个时点有人会去使用。下方的价格投机则是连接矿工和用户的桥梁，即账簿的代币因为右方用户需要产生了价格，而左方矿工通过有价代币将代币激励落到实处，价格投机者则为双方将价格流动性坐实。

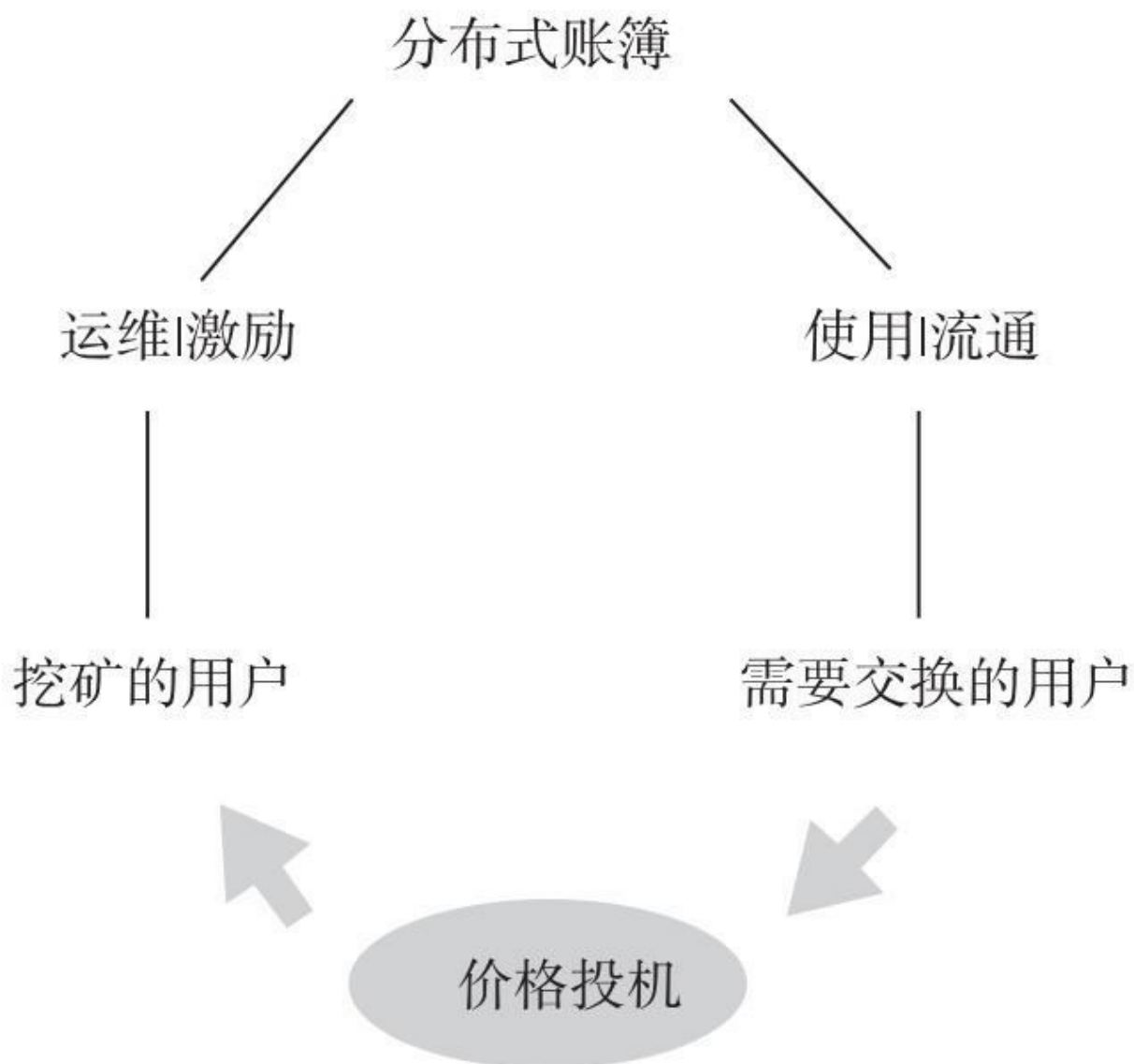


图8-1 PoW机制下的区块链运作机制

在以上运行机制里任一环节都必不可少。缺少了挖矿，系统没有了记账人无法运作；缺少了用户，系统代币无法产生价格；缺少了价格投机者，代币价格缺少流动性矿工激励不足。反之每个环节都各司其职的话，理论上来说图8-1可以形成一个闭环，也就是形成了一个纳什均衡。[\[54\]](#)

纳什均衡有一个很重要的特点，即信念和选择之间的一致性。也就

是说，基于信念的选择是合理的，同时支持这个选择的信念也是正确的。所以，纳什均衡具有预测的自我实现（self-enforcement）特征：如果所有人都认为这个结果会出现，这个结果就真的就会出现^[55]。中本聪有类似的观点，他说比特币就是一个自我实现的预言。

理论上，信念和选择之间的一致性自我实现特征，使区块链可以像永动机一样稳定运行。然而永动机真的永动吗？仔细观察图8-1便会发现该永动机始终还需要燃料，燃料首先便是用户对于账簿的持续性使用的需求，其次是价格投机的需求。

实际上情况是，由于区块链代币的强交易品特性，使图8-1下方的价格投机和真正的用户需要往往混在一起，难以分辨（更不用说矿工本身也是价格投机的常客）。先把比特币放一边，可以发现近年来诞生的大部分区块链代币存活过两年的比例很低。这个事实可以说明想要单纯依靠价格投机的需求实现区块链运行的纳什均衡几乎是不可能的。区块链的运行始终还是需要能够满足真正的用户需要，提升用户使用需要的效用。

回到本节开篇的问题：区块链到底是贵还是便宜呢？我的答案有些取巧：只要能够真正提升用户的边际效用，那么不管多贵的区块链都是便宜的。

四、比特币的内在价值：当它成为一种刚性需求

自从比特币出现价格后，质疑之声就不绝于耳。好听一些的有格林斯潘和诺奖得主罗伯特·席勒说比特币没有内在价值，是泡沫。难听一些的就直接说它是庞氏骗局，是传销。果真如此吗？下面将对比特币的价格构成进行拆解分析，看看它的内里到底有没有什么价值。

比特币诞生至今也不算长远，不到8年的时间。让我感到不可理解的是，当质疑者们讨论比特币有没有价值的时候，仿佛都在讨论一个形而上的东西，例如法币、内在价值等，却很少有人愿意看一看这几年间除了价格图表和舆论口水实实在在的发展历程。

第一个例子：2011年开始伴随着网络黑市“丝绸之路”的快速发展，比特币作为其唯一的支付手段价格开始水涨船高。价格上涨的原因很简单：

- ①互联网上有人需要买丝绸之路上的东西，例如毒品、枪支；
- ②有人也想卖；
- ③没有一种互联网上的跨国支付手段（例如VISA）可以，或者说愿意接入丝绸之路，因为它是黑市；
- ④比特币是跨国的，同时不需要有机构“许可”即可接入；
- ⑤比特币因此被买卖双方需要了，而且还是客观上的垄断性需要。

第二个例子：维基解密。VISA和MasterCard于2010年12月停止维基解密的捐款支付通道，此后Paypal和西联汇款也加入该行列。迫于财务压力，维基解密于2011年开始支持比特币捐款。那么对于想要支持维基解密的互联网公民来说，比特币成为一种刚性需要。

第三个例子：越来越多的劫匪开始拥抱比特币。迫于劫匪的压力，纽约警方都曾在市场上大量购入比特币交赎金。此外，也有越来越多的木马程序开始加入比特币元素：“往×××地址打入一个比特币，否则你电脑里的文件将被删除。”此时比特币对于警察和受害者也是一种刚性需要，而他们既不是自由主义者也不是极客，对于改变世界的金融秩序更是毫无兴趣。

看，这不就是比特币的内在价值吗？

黄金有内在价值，因为它在某些工业上的消耗需要是不可替代的。同时其作为饰品的需要虽然糅杂了投资和消费，其内在价值却是消费的需要——如果买入某一件物品是为了卖出获利的话，这就不是内在价值。大豆的内在价值是粮食裹腹，咖啡的内在价值是提神醒脑，汽车的内在价值是高效的移动，这些最后都会落到人的非投资需要上。和以上物品一样，比特币的内在价值也不是交易市场里的投资或投机，而是来自于刚才说的那些需要。

就像所有大宗商品一样，我以为比特币的价格构成就像一个鸡蛋，蛋黄是其内在价值，蛋清则是价格投机（图8-2）。

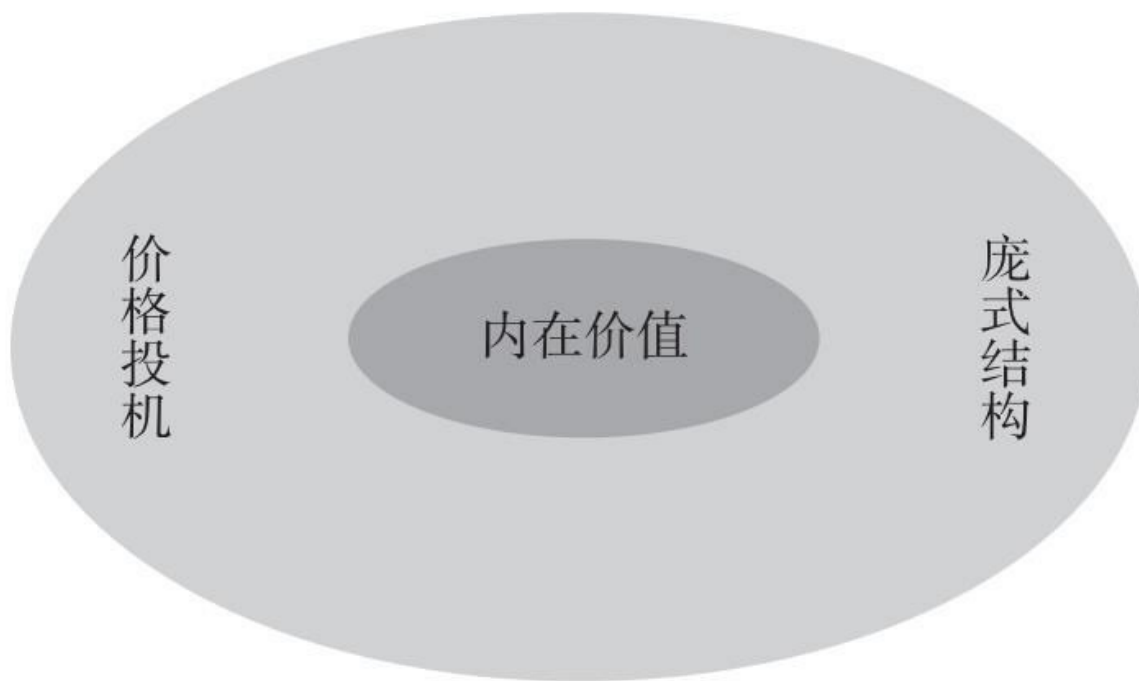


图8-2 比特币价格构成

单纯依靠内在价值也能产生价格，只是比特币作为商品来说天生又是一个交易品（对于买方来说只是购入了比特币，但是对于丝绸之路卖家、阿桑奇、劫匪这一方来说迟早也会卖出，而窍门正是在于“迟早”两

字），所以其价格自诞生之日起就包含着内在的消费性需要和外在的价格投机，无法分开。由于作为其价格蛋清组成部分的投机资金占据了更大的比例，这种构成导致了比特币价格长久来看都会是巨幅波动的。

另外要提一句，庞式结构不等于庞氏骗局。庞式结构出现在所有交易品上，股票、大宗商品、黄金、外汇，甚至房产的价格里都有庞式结构存在[\[56\]](#)。交易品的价格就像行驶在大海中的帆船，船上的人们时不时都会被大大小小的旋涡——庞式结构——所影响甚至是卷入。

五、博弈与合作：区块链——信任的机器

2015年11月，《经济学人》刊登了区块链主题的封面文章：信任的机器。信任是什么？信任是一座被云雾覆盖看不到桥面的桥，连接着合作双方。想要合作吗？行，走过桥来。看不到桥面怎么办？不知道对方怎么想的怎么办？选择吧，相信或者不相信。人们为了此次的合作和将来的合作，在选择之前和选择之中和选择之后不断进行着信息的交换和反复的博弈。

信任是什么？信任是一种预期和期望。人们通过信息的收集和自主的判断，对于某项事件的发生（尤指合作）进行概率的判断。是100%，50%，还是10%？[\[57\]](#)刚才的那座桥就是博弈中的不完全信息，而对于桥对面的人内心想法的猜不透便是博弈中的不完美信息。但是人们始终还是要判断，要去信任，否则人类社会就没有合作，就没有发展。

区块链这个机器通过数学、代码和经济使一些过去发生的记录不可更改甚至牢不可破，这是其一。它还通过智能合约将合作的约定写在区块链上一方面无法更改，另一方面区块链在将来条件触发之时也会自动执行，这是其二。

可以这样去理解区块链的第一个特点“不可更改”。不可更改意味着信息的可信，如果乙方主动提出将区块链上的数据给予甲方，那么其他条件不变至少甲方会更信任乙方和乙方的数据一些。可能甲方本来对于乙方非区块链数据的信任是50%。那么当甲方看到乙方愿意给出区块链数据之后，甲方可以认为由于这些数据造假的难度更高，也就是说虽然仍有造假的可能但是由于区块链提升了乙方造假的机会成本，甲方可能会对乙方数据的信任提升到60%。区块链的数据还有一个特点，即历史越长，造假成本越高。这是因为区块链的数据可以很方便的回溯到此前任一时点。另一方面和一般数据一样的，数据产生的历史交互越多，该数据造假的成本也就越高。所以这时候甲方如果看到乙方给出的区块链数据有10年的历史，而且经过多方使用留下数字签名，那么甲方可能就会对乙方的数据信任提升到80%。这便是第一个特点“不可更改”。

要理解区块链的第二个特点“智能合约”，就要先了解一下博弈论中最基础也是最耐人寻味的“囚徒困境”。囚徒困境讲的是人类在某些合作情况下个人理性与集体理性产生背离。这被认为是人类合作发展的悖论：既然从个人理性和天性出发最优选择总是不合作，那么人类又为何总想着去合作呢？囚徒们彼此合作，可为全体带来最佳利益（无罪开释），但在无法沟通的情况下，因为出卖同伙可为自己带来利益（缩短刑期），也因为同伙把自己招出来可为他带来利益，因此彼此出卖虽违反最佳共同利益，但却是自己最大利益所在。但实际上，执法机构不可能设立如此情境来诱使所有囚徒招供，因为囚徒们必须考虑刑期以外的因素（出卖同伙会受到报复等），而无法完全以执法者所设立之利益（刑期）作考量。解决囚徒困境一般理解有三种方式：第一，订立具有强制力的契约、合同等；第二，重复博弈；第三，教育。[\[58\]](#)智能合约想要实现的便是通过订立具有强制力的契约、合同，解决囚徒困境。

智能合约初看似乎很好，没有问题，细细想来却有很多疑问。一方面具有强制力的契约与合同，似乎已经在社会上普遍存在；另一方面脱离了现有的国家机器，智能合约真的能够实现强制执行吗？

要回答这两个问题，就需要先退回来看一看现行的信任体系是怎么样的。一般认为现行的信任体系来自于两个方面：国家机器和文化传统。

国家机器是对国家层面进行公信力和公权力的背书，在国家的法律法规以外，民间签订的合同也都有对应的法律条款进行约束。相比国家机器的直接明确，文化传统则更软性，主要体现在一些隐形的规则之上。例如，证券公司需要根据法律法规对投资者进行T+1的结算，如果证券公司违规没有按时结算，那么国家机器就会采取行动强制其执行结算。而对于温州人来说各种民间小会的投入和结算则由当地的文化习俗所致。文化习俗的信任体系形成相对较慢，相比国家机器而言成本低很多。2016年春晚宣贯的诚信社会就是希望民间的文化习俗向着互信发展，因为单单依靠国家机器的成本太高了，很多地方管不到也管不好。从刚才三种解决囚徒困境的方式看，可以认为国家机器是订立具有强制力的契约、合同；文化习俗则是重复博弈和教育。

但国家机器不是万能的，订立具有强制力的契约也不是万能的。原因很简单：社会很复杂，事事都要签订契约太麻烦，国家机器在强制执行层面的成本也太高。成本达到一定程度后的结果就是管不了。那么智能合约在这里是不是刚好可以帮助国家机器节约成本呢？如果说要用来填补国家机器空白的话，又如何实现智能合约的强制执行呢？

如前所述，区块链机器具有不可修改和不可逆的特性，以工作量证明机制为例，计算力决定了它数学上的合法性。在国家机器触手无法触及的领域，可以依靠智能合约和数字货币实现自动化执行。此处货币为广义上的货币，即一种价值共识，可以是货币，也可以是信用甚至可以是双方之间独有的价值共识。当智能合约将甲乙双方的价值共识（当然也包含狭义上的金钱财货）内置其中，并约定通过区块链进行条件设立以及触发后的执行，就等于是甲乙双方在订立合约时进行了相关的承诺。只要价值共识存在，违约成本就存在，双方理性的情况下，承诺的

效果就不会变。

那么，区块链消除了“可信第三方”又是指什么？现在的主流说法是区块链实现了“去信任化”，通过区块链使人们不必需要信任对方或是可信第三方机构。区块链实现的是一种信任的转移，使人们在合作过程中的信任对象由人和机构转移到区块链这个共识机器上。

区块链没有消除信任，在合作的过程中人们仍然需要去“信任”一些东西。只不过信任的对象由此前的人和由人组成的机构，转变为共识机制构成的区块链。而共识机制并没有把人性剥离。恰恰相反，共识机制的基础正是人类最为理性纯粹的经济人假设中的逐利特性，辅以密码学以及代码作为封装，再通过互联网和参与者的共同偏好将传播的成本尽量最低。可以认为区块链所做的事情是，先找到人类共有的共识：逐利并通过共识机制收拢，然后告诉具体的博弈双方：别猜了，相信其他人的共识吧，最后具体博弈双方完成博弈合作。当所有使用区块链完成合作的人所获得的集体效应超过维系区块链所需要的成本之时，其应用就会不断发展壮大，也会通过更多的合作增加人类社会的福祉。

[49] 本章由陶荣祺写作完成。陶荣祺，小蚁Onchain VP，上海国际金融研究中心特约研究员，巴比特专栏作家；多年银行、银联、第三方支付及数字货币行业从业背景；《区块链新经济蓝图及导读》译者之一。

[50] 世界上的各类数字货币交易所交易量虽然不断呈上升趋势，可在世界范围被认可的多币种交易所。多币种交易所也被称作“山寨币交易所”或“数字资产交易所”。典型的多币种交易所如Poloniex.com，其以比特币作为基准交易货币，拥有百余个交易品种。同时近年其门槛也有了相对的提高，也就是说某种数字货币要想进入全球交易市场也并不是随心所欲就可以实现的。

[51] Bitcoin Improvement Proposals，基于社区的比特币改良建议。

[52] 比特币虽然有基金会但其口碑与影响力一般，故定其为社区主导。

[53] 或许最近结合量子理论的脑科学告诉了我们答案：人的行为是随机的。

[54] 区块链运行的纳什均衡的定义是：当所有其他人都不改变策略时，没有人会改变自己的策略，则该策略组合就是一个纳什均衡。

[55] 张维迎.博弈与社会 [M].北京：北京大学出版社，2014.

[56] 关于庞式结构的定义和介绍见乐平：《信用、支付和流动性——金融危机结构观察》。

[57] 该定义取来以太坊创始人Vitalik Buterin的Blog“Visions, Part 2: The Problem of Trust”。

[58] 来自耶鲁大学本·波拉克（Ben Polak）教授的公开课。

后记

长铗

如果用一件事物的发明来类比区块链的诞生，我会选择印刷机。印刷机影响了历史的进程，进而影响人们对资源与交易的认知。

在印刷机诞生之前，人们处理知识的方式就是处理竞争性资源的方式，比如某本手抄本圣经、兵书或制造工艺手册。印刷机、计算机发明以后，知识不再是竞争性资源，而变成了一种可规模化生产的商品，“所有东西都在变成软件。印刷机诞生后，人类写过多少个字，未来就有多少家软件公司……”^[59]但与之带来的问题是，在数字世界，我们很难防止资源被复制。我们无法像销售土豆一样销售音乐、软件与其他电子资源，除非我们引入可信第三方，寻求他们来管理我们的财富，证明我们的身份，保护我们知识产权，评估我们的信用。然而，区块链的面世有可能终结这一局面。

如果说印刷机的意义就在于将信息资源抽离物理世界的束缚，变为一种非竞争性资源，区块链则是起着与印刷机截然相反的作用，它以处理竞争性资源的方式来处理信息资源（非竞争性），人们可以摆脱对可信第三方的依赖，在数字世界中自由地交换数字货币、知识产权、股权甚至不动产所有权。虽然两者处理资源的方式是相反的，但两者对话语结构的改变是一致的。

在中世纪，教会垄断着知识与教育，普通人没有直接阅读和解释《圣经》的权利，教会能随心所欲地释读《圣经》。同样，行业工会为了垄断商品制造工艺，排斥外来竞争，对制造工艺知识的出版印刷进行严格的控制。那个时候欧洲大多数国家都通过许可制度，对印刷出版进

行严格的管控，而权力则掌握在天主教堂和政府的手中。行业工会则与天主教和政府进行合谋，对工艺知识的出版和流通进行审查。

也许，今天的我们难以理解私自印刷一本《几何原本》怎么会是犯罪行为。可是仔细想一下，中心化的信用管理机构，不正像是中世纪的行会吗？如果区块链技术能够代替第三方完成对信用的管理，甚至管理的更高效、更安全，我们为什么不投身于其中，去探讨另一种可能？

三年前，我与志趣相投的朋友们一道写了国内第一本比特币专著《比特币——一个真实而虚幻的金融世界》。三年后，比特币归于沉寂，一些曾经热血沸腾的朋友也杳如黄鹤渐无音信，所幸，更多的人坚持了下来，从比特币底层技术里窥见了区块链的潜力。于是，这本书有了更多远见卓识的同人加入，他们有学者、研究员、程序员，还有创业者，在各自擅长的领域，如经济、管理、金融、法律、创业实践等，贡献自己的思想与热情……

在组稿过程中，我们并不盲求认识统一，而是主张各自在专业领域自由发挥所长。区块链思想就好比一个多面体骰子，目前有一面已经揭晓，即数字货币，我们都承认比特币是第一个成功的区块链应用，但接下来，掷下的骰子会是哪面？却是个未知数。每个人心中都有一个自己理解的区块链，很难说哪种理解更高明、更深远。正如本书的副标题，一波三折。起初，达鸿飞主张叫“从数字货币到可编程社会”；后来韩锋老师提议叫“从数字货币到信用协议基础”，还有杨涛老师、蒋海提议“从数字货币到价值互联”……

可编程社会侧重的是区块链强大的脚本功能与可扩展性，区块链通过特定的算法来计算出权益、信用与身份的真伪，这些算法以强大的加密技术为支撑，可以根据不同应用场景，灵活编写不同的智能合约。

信用协议基础侧重的是区块链交易不可逆、数据不可篡改的一面。需要指出的是信用在此有两种蕴含，第一层是信任，解决的是交易行为

的诚实问题。工作量证明等共识机制的发明消除了对可信第三方的依赖，通过分布式网络来保障交易的真实可靠，杜绝了双重支付、交易回滚的可能。第二层是信用，解决的是交易对象的诚实问题。区块链信用的真实可靠，可以让两个素昧平生的人彼此交易，或者完成借贷、担保交易等复杂智能合约行为，本质上利用的是区块链时间戳使真实交易行为与刷信用交易行为在概率分布上可区分的特性。

价值互联网侧重的是区块链以处理竞争性资源的方式来处理非竞争性资源的一面，有人说区块链是互联网世界继万维网以来的第二个伟大纪元。如果说万维网实现了信息互联网，把竞争性资源搬到了数字世界，使复制的边际成本无限等于零，那么区块链则实现了价值互联网，可以在数字世界中处理竞争性资源，使攻击者难以承受51%攻击、篡改交易记录的成本。

还有人把区块链理解为共享账簿，欧洲央行和英国政府都发布了关于共享账簿的报告，侧重的是区块链作为分布式记账的一面，旨在从政府职能与不同利益集团的角度，改善自身业务流程与服务公民、用户的质量，提高金融市场、供应链、电子商务以及上市公司注册等领域的效率。但将区块链仅仅视为一个分布式的记账系统，是一种买椟还珠式的误解。分布式的记账功能，不过是区块链众多特性中的一个。共享账簿只是看到了区块链在数据库层面的创新，而忽视了区块链在建立信用的互联网协议层面的创新。

《经济学人》则把区块链喻为“信任的机器”，机器是智能合约的形象化，每一个智能合约就像是一个原胞自动机，通过简单的规则，构造各种不同的交易行为，整体上大大优化社会资源的流转效率。区块链将过去我们对权威第三方的信任转化为对算法对数学的信任。但信任仅是信用的第一层蕴含，针对的是交易行为本身，信用机器一词的蕴含更饱满，因为区块链同样可以建立交易对象的信用，一个人的区块链交易历史足以证明他的诚信记录，且这种记录具有专属性与跨平台性。然而即

即使是信用机器的说法，也是不够全面。如潘志彪所指出的，区块链不是一般的机器，大部分机器可以被关掉，区块链却是一个分布式系统，一旦被启动，便无法停机。最终，我们选择“从数字货币到信用社会”这一副标题，因为我们相信随着信息互联网向价值互联网的过渡，区块链终将润物细无声，深入到社会的方方面面。

区块链是一种思想，是许多个开源项目的集合，也是无数头脑风暴的“总账”，技术会被淘汰，发明会过时，公司会倒闭，但分布式思想不会。正如印刷机的诞生一举瓦解了中世纪行会、教会对知识的垄断，重塑了社会权力结构，区块链技术也将从根本上改变今天我们对资源与交易的理解，改变政府、公司与个体参与经济行为的方式。托克维尔在《美国的民主》中说：“枪炮的发明使奴隶和贵族在战场上平等对峙；印刷术为各阶层的人们打开了信息之门，邮差把知识一视同仁地送到茅屋和宫殿前。”那么现在，时代可以为这段话添加新的注脚：区块链为我们启动了信用机器，让政府、公司、机构与个体作为平等的节点呈现在分布式网络上，各自管理自己的身份与信用，共享一部不可修改的交易总账。

虽然区块链技术自身还不完善，就像是一个粗陋的玩具，但不要忘了1876年电话发明时，人们是怎样评价的。在当年西联电报公司备忘录里还写着：“电话这个东西毛病太多，并不是一个值得考虑的通信方式，基本上对我们没有什么价值。”

[59] 阮一峰在《黑客与画家》中介绍保罗·格雷厄姆（Paul Graham）时引用的一句话。

附录

附录1 国内区块链项目一览表

序号	项目名称	项目类型	项目简介	地区	官网链接
1	巴比特	区块链综合服务	巴比特建于 2011 年, 目前是国内人口级区块链/数字货币基础信息与数据服务平台, 旗下包括巴比特资讯、巴比特社区、区块元、币众筹四大产品。巴比特资讯 (www.8btc.com) 的定位是给用户提供全视角的全球区块链/数字货币金融新闻与信息, 聚合区块链意见领袖, 推进区块链前沿技术、商业应用、政策监管方面的研究; 巴比特社区(8btc.com) 的定位是为区块链开发者、创业者、投资者提供一个高质交流分享平台, 目前已为业界 40 余个区块链创业项目建立专门讨论区, 帮助他们获取种子用户, 加速产品迭代更新; 区块元(blockmeta.com) 是巴比特创新型产品, 定位是为比特币业界提供区块链交易记录查询、数据挖掘、交易标识、地址监控等服务; 币众筹(bizhongchou.com) 专注于区块链垂直领域的融资众筹, 支持比特币/人民币两种支付形式与回报型/股权型两种众筹模式, 目标是通过闪电网络与侧链技术建立股权众筹区块链解决方案, 在区块链上实现股权众筹的登记发行、转让、清算等金融业务。	杭州	http://www.8btc.com/
2	比特大陆	区块链基础设施	北京比特大陆科技有限公司(Bitmain) 是一家专注于高速运算芯片研发的高科技公司, 曾成功设计并量产多款具有全球领先水平的数字信号处理领域的芯片及整机系统, 拥有最先进的 16 纳米制程的全定制设计经验, 在业界享有盛名。自此之后, 比特大陆不断投入研发在数字货币、区块链、人工智能、新能源等前沿科技领域, 并成功兼并收购和投资赞助了多家国内外创业公司及团队, 成为行业内首屈一指的跨国企业。Braftchain 是比特大陆内部孵化的区块链创新项目, 是基于研发的 Braft 共识算法运行的联盟链, 兼容以太坊平台的智能合约, 提供区块链定制等技术服务。	北京	http://bitmain.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
3	布比区块链	区块链开发平台	布比公司专注于区块链技术和产品的创新,拥有多项核心专利技术,例如:可数学证明的分布式共识技术、快速的大规模账本存取技术、支持业务形态扩展的多链总账技术、异构区块链间的互联技术等;开发了高可扩展高性能的区块链基础服务平台,具备快速构建上层应用业务的能力,满足数千万级用户规模的场景,能够快捷、可靠、安全地基于布比区块链构建大规模商业系统。当前,布比区块链已经广泛应用于贸易金融、股权、供应链溯源、积分、信用、数据安全等诸多市场领域。以多中心化信任为核心,致力于打造新一代价值流通网络,让数字资产都自由流动起来。	北京	http://www.bubi.cn/
4	OnChain	金融服务	Onchain 开发了中国首个区块链项目——小蚁。小蚁是一个用于登记数字资产的区块链底层协议。通过小蚁,资产拥有者可以把各种实体世界的资产进行数字化,变为流通在小蚁区块链上的数字资产,从而进行流转和交易。小蚁的代码完全原创,是国内唯一实时开源的区块链项目。小蚁的一个应用方向是用于非上市公司股权的发行登记和流转交易。Onchain 另一重要业务是企业级区块链解决方案——Onchain Solutions。Onchain Solutions 以小蚁的代码为基础,通过与 UCloud、微软 Azure 等云计算平台合作,以 Blockchain-as-a-Service 的方式向企业用户提供联盟链、私有链的开发、部署、运维服务。	上海	http://www.onchain.com/
5	银链科技	区块链开发平台	银链科技的区块链公共技术开发平台是开放、开源的区块链底层技术平台,以便金融机构广泛采用,在其上开发各种应用,形成事实上的区块链标准。银链科技还将为金融机构提供整套区块链技术解决方案,提供商业化咨询、培训、开发或外包服务。	深圳	http://bankledger.com/
6	区块元	数据服务	区块元是巴比特旗下区块链数据与区块链底层技术开发服务平台,目前为国内最大第三方区块链数据驱动引擎,为投资者、交易者、开发者提供区块链查询、数据挖掘、交易标识、地址监控等多元服务。立足于第三方中立节点,研究与开发私链、联盟链、公有链的通信协议,实现标准化加可定制化的企业级 SaaS 服务。	杭州	http://blockmeta.com/

7	火币	数字资产交易	火币网是中国最大的数字资产交易平台之一,获得红杉资本等机构 A 轮 1000 万美元投资,为全球 30 多个国家和地区 150 万注册用户 提供数字货币交易服务,执行严格风控管理,稳定运行 3 年。截止 2016 年 5 月,火币网累计成交额达 9000 亿元,连续 7 次刷新全球比特币最高交易记录。	北京	https://www.huobi.com/
8	OKCoin	数字资产交易	OKCoin 是全球知名的区块链资产交易平台,拥有来自 100 多个国家的用户。OKCoin 拥有业内专业的开发技术团队、金融产品团队和技术安全专家,致力于为投资者提供安全、快捷、稳定的区块链资产交易。OKCoin 率先使用区块链技术与资产发行单位合作,发行区块链资产,实现区块链资产的全球交易。	北京	https://www.okcoin.cn/
9	BTCC	数字资产交易	BTCC 最初以“比特币中国”的名字创立于 2011 年。是中国第一个比特币交易所,也是目前全世界运营历史最长的比特币交易所。如今,BTCC 引领着比特币生态圈的各个方面,提供数字货币交易所、矿池、支付网关、用户钱包和区块链刻字等服务。BTCC 在一个综合平台提供不同的产品和服务,方便全球用户能全方面地参与数字货币领域的所有环节。	上海	https://www.btcc.com/
10	邻萌宝	其他应用	邻萌宝是全球首创的基于地理信息(LBS)和移动互联网生态的区块链数字资产系统。同时,邻萌宝又是第一个将真实线下商家引流的需求和游戏娱乐方式的玩家参与,以及区块链数字货币结合起来的移动 APP 应用。在邻萌宝中,玩家在地图和现实中探索,即可获得数字货币 LMC 和商家优惠等双重实惠,而商家则赢得了玩家实地到店的高价值的真实 O2O“流量”,创造了全新的玩家和商家之间的价值交换以及流量变现通道。	北京	http://www.lomocoin.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
11	雷盈量化投资管理	金融服务	雷盈是数字资产领域的金融科技服务提供商,专注于区块链大数据挖掘与研究、人工智能在投资与资产管理领域的应用,为专业机构和用户提供数字资产管理整体解决方案。雷盈结合区块链大数据挖掘与人工智能,依托于高性能的精算系统和分布式运作系统,引领了数字资产管理的智能化变革,为专业机构、企业和高净值客户提供区块链金融大数据服务、数字资产行情趋势分析、数字资产量化投资技术支持、数字资产投资管理与定制化市值管理等一系列服务与产品。	上海	http://radarwin.com/
12	Vechain 唯链	防伪公证	Vechain 是一个基于区块链定制化 NFC 的商品防伪平台。系统应用非对称加密算法集成的 NFC 芯片作为商品的唯一无法复制的标识,将区块链作为正品的公钥储存平台。这个项目将以奢侈品作为首先切入的行业,从而再深入的酒业,食品安全以及医疗卫生。平台使得每一个商品都对应的有一个唯一的 ID,每一个区块链上储存的 ID 对应唯一的一个商品,从而形成一个全球化的透明的供应链平台,在这个平台上生产商、渠道商、零售商、海关、商检、用户,所有角色同时接入,生产、分发、物流、销售、审验、消费,所有环节同时记录。	上海	http://www.vechain.com/
13	ODIN (PPkPub)	区块链基础设施	ODIN(Open Data Index Name) 是开放数据索引命名标识的缩写。广义上,ODIN 是指在网络环境下标识和交换数据内容索引的一种开放性系统,它遵从 URI(统一资源标识符)规范,并为基于数字加密货币区块链(BlockChain)的自主开放、安全可信的数据内容管理和知识产权管理提供了一个可扩展的框架。它包括 4 个组成要素:标识符、解析系统、元数据和规则(Policies)。狭义上,ODIN 是指标识任何数据内容对象的一种永久性标识符。	北京	http://ppkpub.org/
14	HaoBTC 好比特币	金融服务	HaoBTC 是全球领先的比特币钱包平台,提供便捷、安全、专业的比特币交易服务,7×24 小时自动充值,秒级交易。同时作为最好的比特币钱包,采用 SSL、HSM、MULTISIG 等机制,确保存币、发币和收币的安全流畅。	北京	https://haobtc.com/

15	朝夕网络	综合服务	朝夕网络提供一站式解决区块链专家顾问服务,一站式区块链技术解决方案服务,也为非营利性机构提供免费咨询培训服务。	上海	http://zhaoxi.co/
16	果仁宝	区块链开发平台	果仁宝,是以区块链技术为基础,以用户为中心的全球数字积分服务平台。目前主要为游戏,电商,视频等行业提供积分消费解决方案。果仁宝产品是基于 Goopal Blockchain 技术衍生而来的应用。在未来,一方面建立 Goopal 平台,开发者可以通过极低的门槛使用 Goopal Blockchain 技术;另一方面积极与寻求区块链技术支持的企业或组织建立商务合作,在为其提供技术解决方案的同时丰富 Goopal Blockchain 的应用场景,逐步构建 Goopal Blockchain 生态系统。	北京	https://www.goopal.com.cn/
17	区块	数据服务	区块提供区块链数据查询、统计等基础服务,同时专注于区块链基础理论与基础设施的搭建。	北京	http://qukuai.com/
18	维优区块链	综合服务	维优区块链专注于为专业客户、金融机构和政府部门提供资产数字化解决方案,维优团队集合了区块链行业的顶尖咨询顾问与专家、最具执行力的技术开发精英和市场先锋。维优以专业服务为客户解决资产数字化、场外资产和非标准化资产在公开市场的流动性问题,让用户在数字资产的托管、确权、转移和交易等过程中体验到技术带来的操作安全性和便捷性。	上海	http://www.viewfin.com/
19	云币	数字资产交易	云币网由李笑来投资,创立于2013年6月,是采用自主开发的开源程序搭建的区块链资产交易平台,已经安全运行3年。云币网着眼于世界区块链行业发展趋势,将平台定位为区块链资产交易枢纽,以真正有应用价值为核心特征来引入更多有投资价值的区块链资产上线,为用户提供区块链时代更多更好的投资机会。	北京	https://yunbi.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
20	智能坊	智能合约	智能坊是一款真正意义上的第二代数字货币系统,该系统旨在实现为第三方开发者提供图灵完备的 C/C++ 语言作为合约开发语言,大大拓宽了数字货币的应用领域,并有效降低了开发者在数字货币区块链上进行各类去中心化应用的开发难度。	深圳	http://www.dacrs.com/
21	币区势	金融服务	币区势为数字货币投资者提供专业的实时行情大数据分析服务。主要发展方向是社会化大数据挖掘,区块链大数据挖掘,基于大数据的量化交易、智能投顾等。目前已研发了“多空指数”“新人指数”“情绪指数”三个指数,研发的指数短线和中长线兼备,场内场外数据相结合。数据已经应用到实践当中,并获得大量用户的认可。	广州	www.biqushi.cn
22	OKLink	金融服务	OKLink 是 OK Inc. 于 2016 年推出的构建于区块链技术之上的新一代全球价值传输网络(blockchain transfer network),致力于通过区块链技术推动普惠金融的全面发展,重塑金融体系架构。OKLink 联结全球中小型金融参与者,包括银行、汇款公司、互联网金融平台等,借助区块链技术极大提高价值传输网络的速度、成本及安全性。该网络已有遍及全球的数十家合作方加入。	北京	https://www.oklink.com/
23	SFARDS 理安科技	区块链基础设施	理安科技成立于 2014 年,由前世界著名挖矿芯片和矿机厂商 Gridseed 与全球第一个开源挖矿管理软件 Wiibox 团队合并而成,并获得经纬中国 A 轮投资。SFARDS 研发诞生了全球第一颗 28nm 工艺的比特币莱特币双算法芯片,迄今为止也是唯一一颗多算法挖矿芯片。目前主要从事基于自有知识产权的区块链挖矿芯片、硬件和软件产品在各行业区块链及智能合约应用的开发、推广和运营。	北京	http://www.sfards.com/

24	Qtum OS	区块链基础设施	Qtum OS 是全球第一个区块链环境操作系统,是基于 Linux 核心的深度定制化的一套方便使用的,灵活的,安全的一站式开发及运行环境,同时也是为个人或者企业提供一个开发 DAPP 以及搭建 DAO 的基础环境。目前在这个环境里可以即插即用的运行及开发基于 Bitcoin, Ehtereum, Bitshare 的各种应用。Qtum OS 对文件系统做了特殊处理,使得文件不会因为终端被黑客攻破而全部暴露在黑客的眼前。同时 Qtum OS 也专门在定制了相应的区块链编译器。今后将会为企业及个人无论开发和运行公有链还是私有链都提供一个安全可靠方便的平台。	上海	http://bitse.com/
25	比太钱包	区块链基础设施	比太钱包是 Bitcoin.org 官方推荐的比特币钱包,是易用安全的比特币及其它区块链资产的管理方案,能让用户轻松的实现大额资产的冷存储和小额资产的热管理,保护了很多个人和企业的比特币及其它区块链资产。	北京	https://bither.net
26	币定行	区块链基础设施	佛山市币定行科技有限公司致力于设计研发最优质的比特币交易设备,为商家提供系统的,易用的、安全的、并且是去中心化的交易解决方案。2014 年 06 月,启动硬件钱包(BWallet)项目,2015 年 01 月 BWallet 正式发售。	佛山	https://www.bidingxing.com/
27	反应链科技	综合服务	成都反应链科技有限公司主要有三大块业务:1. 天府区块链培训:培养成都本地区区块链的技术和项目开发人才,打造西南地区的区块链创新资源平台;2. 区块链征信应用:使用区块链的防伪、不可更改等特性,应用到企业征信。;3. 区块链资产证券化:资产证券化是一项内容繁杂,流程手续极多的资产运营方式。在其间区块链的不可作假、时间戳等特性可以运用于资产证券化的公证和交易等流程。	成都	http://www.fylkeji.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
28	守诺链	防伪公证	"守诺链"是基于布比区块链技术的存证云服务平台。它起源于“拉勾上钩”朴素的承诺,满足人们生活中对于“承诺”的需求。“守诺链”依靠区块链技术的机密性、不可篡改性,把生活中的承诺、便条、借条、版权、信息披露等数据实时锚定到“守诺链”中完成时间存证工作,用更便捷和安全的手段服务于社会生活的存证业务;如遗嘱订立、电子合同签署、信息的时间留证、保险关系确立、公证业务等。	广州	暂无网站
29	嘉楠耘智 Avalon	区块链 基础设施	Avalon 项目致力于为数字区块链领域提供性能更加卓越的计算设备及相关配套服务。Avalon 项目的产品已经销往全球超过 150 个国家和地区,售出芯片的算力一度占到全球区块链共识计算网络的 30%。Avalon 项目所在的嘉楠耘智信息科技有限公司自始至终对 Avalon 项目保持着极高的研发投入,使得其数字区块链计算设备的核心——超算芯片,以每年 1-2 代的速度快速进行迭代。	杭州	https://ehash.com
30	Bitbank 比特银行	金融服务	Bitbank 是一家虚拟货币银行,为客户提供全面、专业的虚拟货币理财服务。业务内容具体包括:储蓄业务,包括比特币和莱特币的活期储蓄、定期储蓄;P2P 借贷理财,包括比特币及莱特币的借贷理财;虚拟货币挖矿理财;比特币云算力理财;目前仅提供比特币、莱特币的交易,平台未来还将增加其他稳健虚拟货币的理财产品。为了顺应潮流的发展,抓紧新一代科技带来的机会,Bitbank 在 2015 年末成立了区块链研究院,致力于区块链技术的研究和宣传普及。	深圳	https://www.bitbank.com/
31	BitBays	数字 资产交易	Bitbays 为全球超过 80 个国家的客户提供给予美元和人民币的虚拟货币兑换服务和未上市公司虚拟股权登记与交易。其创新的多币种钱包可进行支付,虚拟货币兑换和申购虚拟货币套利基金等功能。	北京	https://bitbays.com/

32	Cryptape	区块链 开发平台	Cryptape 多数成员拥有 10 多年的软件开发经验,提供技术咨询服务超过 6 年,有着丰富的产品研发经验和完整的技术储备。公司多数成员 11 年开始接触比特币,14 年团队创业,参与开发了全球第一个开源的数字货币交易所“貔貅”;15 年 5 月为杭州安存开发电子数据保全的区块链解决方案。公司为金融,物联网等行业提供区块链相关的底层产品和技术咨询服务,将于 16 年发布国内第一个以太坊兼容的联盟链原型产品。除了联盟链的软件产品,公司还在研发 DApp 应用,并积累了一定的技术储备。	杭州	尚未上线
33	EthCloud	区块链 开发平台	EthCloud 是一个容易使用区块链云计算平台(BlockChain as a service),可以在医疗、教育、数据安全、去中心化存储、财务审计、投票、保险、智能合约等领域,为开发者提供基础服务,促进开发效率,降低区块链的使用难度,让开发者尽快推进区块链的行业应用。	成都	http:// www. ethcloud. cn/
34	保全网	防伪公证	保全网是基于区块链的电子数据存证平台,通过将电子数据 hash 到比特币区块链中用来确保电子数据不可篡改和抵赖,同时保全网跟公证处和司法鉴定中心合作能出具有法律效力的公证书或司法鉴定文书。保全网能为用户提供电子数据存证、电子签名一体化的解决方案。	杭州	https:// baoquan. com
35	太一科技	区块链 开发平台	北京太一云科技有限公司是新三板第一家区块链上市企业,构建了自主知识产权的太一区块链应用体系,立志在中国区块链产业化进程中,为各个行业互联网应用层提供稳定的区块链基础设施、便捷的中间工具和可靠的解决方案。	北京	http:// taiyi - tech. com/

序号	项目名称	项目类型	项目简介	地区	官网链接
36	数贝荷包	金融服务	比邻共赢公司与布比公司合作推出的数贝荷包,是基于区块链技术与理念的联盟方式积分平台。数贝荷包平台中的各个商家是平等的,商家基于对区块链技术的认可,而信任“数贝荷包”平台,那么他们能够主动策划发行自己的积分,并按市场原则接收他家的积分,形成一个积分跨域流动的共享共赢生态。这种积分生态能够充分发挥出积分增强客户粘性、促进消费行为的作用。一旦投入运行,其运转生效就不会被某个成员控制。	北京	http://www.belink.com/
37	币看比特币	综合服务	币看是一款比特币应用工具平台。它是币看网(http://btckan.com)发布的官方应用,是目前中国用户量最大的比特币手机 APP 之一。拥有独特的比特币的 OTC 场外交易功能,同时也提供价格监控、新闻资讯、挖矿监控、股票监控、钱包等服务。	深圳	https://btckan.com/
38	BW 币网	区块链基础设施	币网由全球最大矿机厂商龙矿科技和中国最大比特币交易平台之一中国比特币联合创立于 2014 年 8 月,致力于为比特币用户提供专业、简单、高效、安全、值得信赖的挖矿设备及服务体验。币网的业务涵盖比特币矿机芯片研发、比特币矿机制造销售、比特币矿池、比特币云算力、比特币理财等领域,提供比特币全产业链解决方案。	深圳	https://www.bw.com/
39	格格积分	金融服务	格格积分是全国首个资产型区块链积分平台,与传统积分不同,具有赠送、合并、集中、便利流通以及可以追踪溯源的特点。商家通过发送云贝给用户,达到快速扩散品牌、增加粉丝的效果。商家还可以根据淡旺季设置积分抵换现金的比例,促进营业额的提升。对于用户而言,通过活动或消费获取的积分可以在格格积分平台上全网通兑,不受单一店家、商圈限制,积分还可用于赠送、合并与支付。	中山	暂无网站

40	海枫藤数字资产综合平台	数字资产交易	海枫藤是一个数字资产综合平台,其主要功能是为用户提供各种有资产背书的数字凭证,用户可以在平台上购买、交易这些数字凭证,并享有数字凭证所代表的相应份额的数字资产的一切收益权利。	上海	http://www.bithft.com/
41	物链	供应链溯源	基于区块链的供应链管理云服务:结合供应链的特性对区块链的接口进行继承、封装以及应用扩展,使每一个物品静态(固有特性)和动态(流转、信用)等信息能够在生产制造企业、仓储企业、物流企业、各级分销商、零售商、电商、消费者以及政府监管机构中共享、共识。	北京	暂无网站
42	金股链	金融服务	金股链提供基于区块链技术的股权登记转让服务,为投资人提供高效、可信的资产流通环境和服务。金股链专注未上市公司股权流通服务,以区块链为基础建立全新的股权登记交易模式。金股链以众筹股权登记为出发点,通过与众筹股权市场的合作,逐步建立包括股权登记、认证、转让、交易结算、信息披露等业务的完整成熟的区块链资产流通环境。	北京	http://www.shareslink.com/
43	可零可零	金融服务	可零可零是一个多币种电子钱包 App,用户可以使用它进行多国货币转账、收款和兑换货币,目前只是支持人民币和新台币。可零可零的目标用户包括留学生、海外代购及海淘用户、出入境游客以及一些有跨境业务需求的商家和企业。	北京	https://kelingkeling.com/
44	OXBTC 牛比特	金融服务	牛比特是牛比特团队最新开发的集云算力购买、交易与存币理财为一体的数字货币综合投资平台。数字货币用户可以在该平台上完成云算力购买、二级市场交易,或进行存币理财,获得数字货币投资理财回报。	深圳	https://oxbtc.com

序号	项目名称	项目类型	项目简介	地区	官网链接
45	钱香	供应链金融	钱香金融是上市公司、产业资本和创投基金联袂打造,重度垂直消费产业终端的供应链金融理财平台。钱香现将基于布比区块链技术打造全新的供应链金融服务平台,开展黄金珠宝终端供应链金融服务,基于区块链技术共识、安全、不可篡改的特性,对加盟商的资金用途、进货渠道、还款能力等实现全方位管控,实现金融与供应链物流、信息流的精准融合,为各终端门店提供单笔小额授信,实现资金快速、灵活、低成本运转的普惠金融和供应链金融新模式。	上海	http://www.qianxiangbank.com/
46	F2Pool	区块链基础设施	全球最大的比特币矿池,莱特币矿池,全球第三大以太坊矿池。区块链安全的维护者。	北京	https://www.f2pool.com/
47	水滴互助	金融服务	水滴互助是一个针对重大疾病推出的互助保障平台。其特点是基于场景化大数据和区块链技术,解决用户在面对重大疾病时的医疗资金问题。目前,重大疾病赔付范围涵盖了五十种,全部为癌症。	北京	暂无网站
48	搜搜比特币	综合服务	搜搜比特币是最专业的数字货币行情、资讯、导航平台之一,专注于为数字货币用户提供相关应用与服务的交流平台。拥有优质、全面的数字货币资源,提供专业的数字货币 K 线图,行情应用 APP。每天服务来自全球几十个国家和地区的数万名数字货币爱好者。	深圳	http://www.sosobtc.com/
49	淘贝 ToBay	电子商务	淘贝 ToBay 想要打造一条开放、安全、免费、便捷和去中心化的淘宝链	杭州	尚未上线
50	同心社	金融服务	同心社是一个基于区块链的互助保险项目,包括“重疾无忧互助计划”等产品。为保证互助金征集效率,同心社采取预缴互助模式,如果会员遭遇不幸,其他会员将第一时间予以资助,互助金将从会员的预存账户余额中转出。同时,因为基于区块链技术,所有资金流向是公开透明的,无法伪造和篡改,并且每个用户都可以行使监督的权利。其次,所有资金的划转只能按照公开的智能合约执行,无法人为挪用及干预。最后,每个用户的个人敏感信息都将高度加密,其他人无法查阅。	上海	尚未上线
51	自然经济生态开发插件与管理平台	区块链开发平台	项目以区块链为技术实现方式,建构一个自然经济管理工具与傻瓜式服务平台,让开发者一天内在自己的 APP 中导入自然经济,实现 APP 内自然资产的登记、发行、交易和清算。自然经济为开发者搭建一个集成用户和商家的平台,给商户提供移动端软件开发工具包,简化开发者们在移动端完成去中心化的区块链(认证)记账。	上海	尚未上线
52	信链	区块链基础设施	信链是一个区块链 2.0 的项目,该项目采用新的共识算法来进行实现无需挖矿就可以进行记账,对节点贡献的存储空间和带宽进行激励,可以很好地与存储应用相结合。	北京	http://www.conseweb.org/

附录2 国外区块链项目一览表

序号	项目名称	项目类型	项目简介	地区	官网链接
1	Stem	版权保护	Stem 利用区块链和加密货币技术的创业公司,为内容创作者们提供一个清晰和及时的收入平台。	美国 洛杉矶	https://stem.is/
2	Custos	版权保护	Custos 媒体技术公司是一家南非公司,该公司致力于使用区块链技术打击媒体盗版行为。该公司使用一种能够将比特币水印到媒体中的技术,该技术通过区块链来跟踪识别侵权行为。该系统使用众包向那些识别盗版行为的资源下载者提供奖励。	南非	http://custotech.com/
3	Blockai	版权保护	在 2015 年成立之初,Blockai 被设想为“比特币的 Netscape 浏览器”,当时 Blockai 尝试将区块链变成一种社交媒体流,允许用户发送信息和鉴证产品。现在 Blockai 致力于打造一种新工具,允许艺术家证明或声明自己对图片拥有版权。	美国加利福尼亚州	https://blockai.com/
4	Ownership Technology	版权保护	Ownership 通过利用区块链技术,可以帮助个人和企业保护他们的知识产权。	美国加利福尼亚州	http://ownership.io/
5	Ascribe	版权保护	Ascribe 是一家位于柏林的区块链技术公司,他们通过使用比特币总账系统来保护艺术家的知识产权。艺术家们可以通过这家公司在网上来保护他们的专利,也可以转让和出售他们的知识产权,而不必通过第三方。	德国	https://www.ascribe.io/

6	Ribbit. me	电子商务	Ribbit. me 创建了一个基于区块链的统一客户奖励计划,提供实时奖励回馈和奖励积分换购。高度定制的平台能够在用户确认他们的购买时,尽快执行即时奖励积分。Ribbit. me 允许跨品牌推广活动,以便客户可以使用从其他合作伙伴那里获得的奖励积分。此外,供应商可以根据服务的类型选择积分的归类。例如。住酒店的积分可以与购物积分和航空里程积分分开存放。但是客户可以根据需要,将一种类型的积分转换为另一种积分。	美国 纽约州	http://www.ribbit.me/
7	Simplex	电子商务	Simplex 是一家专注于用信用卡购买比特币的以色列创业公司。	以色列	https://www.simplex.com/
8	Purse. io	电子商务	Purse. io 运行了一个双向的电子商务市场,既提供亚马逊购物者使用比特币支付,并且还提供了很大的折扣,也允许用户用礼品卡来交换数字货币。	美国加利福尼亚州	https://purse.io/
9	Colu	电子商务	Colu 这家公司旨在通过区块链技术来分配物品的所有权,他们的服务可以提供给你一种简单的方式来使用区块链技术。就是可以使用代币(token)来交易任何东西,从汽车,艺术品到演唱会的门票。	以色列	https://www.colu.co/
10	Open Bazaar	电子商务	OpenBazaar 是一个完全使用密码的分布式应用,它允许用户在匿名和不受信的情况下购买和贩卖商品,不需要中央仲裁人,全部使用比特币。	美国哥伦比亚特区	https://openbazaar.org/
11	Chronicled	防伪公证	成立于 2014 年,Chronicled 公司旨在使用“智能标签”来确保消费者产品的真实性,它可以插入鞋子并连接到用户的苹果或安卓应用。然后 Chronicled 会使用区块链技术将鞋子的信息记录在一个分布式账本上。	美国加利福尼亚州	http://www.chronicled.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
12	Civic	防伪公证	Civic 是一家数字身份安全创业公司,重点在于美国社保号的在线安全解决方案。	美国加利福尼亚州帕罗奥图	https://www.civic.com/
13	Stampery	防伪公证	Stampery 利用比特币区块链技术解决了数据的认证问题,它允许个人和公司证明任何类型的数据,生成精确、可靠和不可更改的存在性证明、完整性和所有权。	美国加利福尼亚州	https://stampery.com/
14	Factom	防伪公证	Factom 利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式。Factom 维护了一个永久不可更改的、基于时间戳记录的、区块链数据网络。大大减少了进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。	美国德克萨斯州	https://www.factom.com
15	ShoCard	防伪公证	ShoCard 是一家致力于利用区块链技术来验证身份的初创公司,其将自己定位成可以颠覆数字身份行业的一种角色,它为消费者提供一种安全持有个人身份信息的方式,用户可以无忧地进行在线购物、网上银行登录等。	美国加利福尼亚州	https://shocard.com
16	BlockScore	防伪公证	BlockScore 为客户提供身份证明服务,包括电子商务交易市场,金融机构和数字货币初创公司。	美国加利福尼亚州	https://blockscore.com/
17	EverLedger	防伪公证	Everledger 主要为钻石认证账户及其交易历史提供一个防篡改的数字化分类账,可同时提供认证服务,主要客户为保险公司,同时有助于法律监管实施。	英国伦敦	http://everledger.io/

18	Digix	金融服务	Digix 的目标是建立一个与实物黄金锚定的稳定货币。	新加坡	https:// dgx. io/
19	Bitwala	金融服务	Bitwala 成立于 2012 年,允许用户使用比特币在单一欧元支付区 (SEPA) 转账欧元。	荷兰	https:// bitwa. la/
20	Fluent	金融服务	Fluent 的目标是利用区块链在供应链管理当中的应用,来吸引主流金融公司的关注。	美国 纽约州	http:// fluent. network/
21	Digital Asset Holdings	金融服务	DAH 是由掉期交易所 trueEX 创始人兼 CEO Sunil Hirani 和自营交易公司 DRW Trading 创始人兼 CEO Don Wilson 共同创立的。其目标是成为金融资产交易场所,方便投资者以更低的价格成本和时间成本将传统货币和比特币进行转换。	美国 纽约州	https:// digitalasset. com/
22	Symbiont	金融服务	Symbiont,其起源于 Counterparty (合约币)项目,它是由 Overstock. com 公司旗下 Medici 项目 (现 t0)的前成员创立的,根据 Symbiont 公司的网站介绍,“Symbiont 正在建立第一个用于发行区块链智能证券和交易智能证券的平台。”	美国 纽约州	http:// symbiont. io/
23	Streami	金融服务	Streami 是一家区块链汇款创业公司,他们的主要竞争对手,是传统的汇款服务提供商以及占据韩国对外汇款市场显著份额的非法金钱转移商。	韩国	https:// www. streami. co/
24	Bitwage	金融服务	Bitwage 是目前最大的一家比特币薪酬支付公司,公司获得了 Draper Associates 和 Orange Silicon Valley 的投资。	美国 加利福 利亚州	https:// www. bitwage. com/

序号	项目名称	项目类型	项目简介	地区	官网链接
25	Align Commerce	金融服务	Align Commerce 公司是由前西联汇款总经理 Marwan Forzley 一手创立,该公司正在寻求颠覆小型企业(SMB)的跨境支付市场。Forzley 声称其公司产品改进了传统电汇的跨境交易,这种解决方案带来的不仅是成本上的降低,还有其他方面的益处。	美国加利福尼亚州	https://aligncommerce.com/
26	BSAVE	金融服务	BSAVE 是一家总部位于伦敦的比特币初创公司,为用户提供一个在线存储比特币资产的平台,让用户可直接从自己所持有的比特币资产中获取收益。该公司的目标是从根本上简化在线储蓄和投资的过程,充分开发数字货币的金融服务潜力,为全世界的人们提供便利。	英国伦敦	https://www.bsave.io/
27	Safe Cash	金融服务	Safe Cash 它是一个基于权限许可(permission-based)的区块链,是受银行授权和控制的。Safe Cash 公司银行的技术服务提供商,并不处理任何的钱。此外,因为平台与银行的合作关系,Safe Cash 金钱业务和交易所业务都是特许的。	美国加利福尼亚州	https://safe.cash/
28	BitGold	金融服务	BitGold 是一家总部位于加拿大多伦多的公司,提供了一个专注黄金,以消费者为中心的互联网平台,用于全球区块链支付,同时提供安全,可赎回的黄金存储。	加拿大多伦多	https://www.bitgold.com/
29	Axoni	金融服务	Axoni 平台将区块链技术引进全球市场,充分发挥了去中心化非许可型账本技术的市场优势。	美国纽约州	https://axoni.com/
30	Circle	金融服务	Circle 是一家消费金融公司,专注于通过利用区块链技术来存储和使用金钱,以改变世界经济。	爱尔兰	https://www.circle.com/

31	Skuchain	金融服务	Skuchain 是一家位于加利福尼亚州山景城的创业公司,致力于开发 B2B 贸易和供应链融资区块链应用程序。他们正在开发区块链解决方案,以此来解决价值 18 万亿美元的全球贸易金融市场仍旧依赖纸质文件的问题。	美国加利福尼亚州	https://www.skuchain.com/
32	Zcash	金融服务	Zcash 是一种去中心化的开源加密货币,致力于通过使用突破性的密码学理论提高隐私性的标准。	美国科罗拉多州	https://z.cash/
33	Uphold 尚持	金融服务	Uphold 尚持为用户提供包括比特币在内的其他 20 种法定货币的免费转账、货币兑换服务,创造一个更公平、包容、透明公开以及更具责任感的金融服务系统。比特储创始人哈尔西·迈纳(Halsey Minor)于 1994 年创办了如今家喻户晓的著名科技新闻网站 CNET,堪称是“网络时代奠基人”。		https://uphold.com/
34	BitPay	金融服务	BitPay 由汤尼·各皮(Tony Gallippi)和 斯蒂芬·帕耶(Stephen Pair) 在 2011 年创建,允许企业通过比特币点对点网络实现网络支付。使用 BitPay,一个公司可以接受来自任何国家的付款,即时,零风险,零欺诈。BitPay 同时还提供更方便的汇率交易,把比特币自动兑成商家的当地货币,如美元或欧元,按汇率直接存入他们的银行账户。	美国佐治亚州	https://bitpay.com/
35	Block-chain. info	金融服务	Blockchain. info 是知名 onchain 在线钱包服务商,同时也提供比特币区块链数据查询服务。	卢森堡	https://www.blockchain.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
36	Xapo	金融服务	Xapo 是一家比特币的安全存储服务公司,其 CEO 文斯·卡萨雷斯(Wences Casares)也是比特币领域的早期投资人之一。Xapo 还曾被纽约时报的作者纳撒尼尔·波普尔(Nathaniel Popper)赞为有发展潜力的优秀公司。2014 年,Xapo 累计融资总额已达 4000 万美元,投资方包括 Greylock Partners、Index Ventures 等知名投资机构以及雅虎创始人杨致远等知名投资人。	美国加利福尼亚州	http://xapo.com/
37	Coinkite	金融服务	Coinkite 是一家位于加拿大的比特币企业,提供比特币和莱特币钱包,和支付终端的服务。支持法定货币包括美元、人民币、欧元、加元、英镑、波兰兹罗提、俄罗斯卢布、澳元、日元、巴西币、瑞典克朗等。	加拿大多伦多	https://coinkite.com/
38	BitX	金融服务	BitX 是一家新加坡比特币公司,主营比特币钱包支付业务,在非洲、东南亚、东欧和拉丁美洲都有市场,其中南非、纳米比亚和肯尼亚等地区的比特币交易量都非常活跃。2015 年,BitX 获得 400 万美元 A 轮融资;腾讯第一大股东 Naspers 集团领投。	新加坡	https://bitx.co/
39	Linq	金融服务	Linq 是纳斯达克采用区块链技术推出的新平台,,该平台将促进其私人证券市场的股份以一种全新的方式进行转让和出售。目前,包括 ChangeTip、Chain、Peernova、Synack、Tango 和 Vera 这 6 家公司,已成为了 Linq 平台的内测项目。	美国	http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326
40	i0	金融服务	i0 是 Overstock.com 占有多数股权的子公司,致力于开发和商业化基于加密安全和去中心化账本(俗称区块链技术)的金融技术。自 2014 年 10 月成立以来,i0 已经率先通过整合区块链技术为资本市场带来了更高的效率和透明度。Overstock 将要发行的证券将会在 i0 平台上进行交易。	美国	https://i0.com/

41	Bitshares 比特股	金融服务	比特股是一个基于区块链技术的金融服务平台和开发平台。任何个人和机构都可以在此平台上自由的进行转账、借贷、交易、发行资产和发行自己的智能货币、期货品种等,也可以基于这个平台快速搭建出去中心化、低成本、高性能的虚拟币/股票/贵金属交易所、杠杆期货交易所、承兑网关、资产管理平台(众筹)等。	美国	https://bitshares.org/
42	Ripple 瑞波	金融服务	Ripple 提供全球金融结算的解决方案,致力于最终使世界可以如交换信息一般交换价值——实现价值网络(Internet of Value, IoV)。Ripple 解决方案使得银行之间无需通过代理行,而是可以直接转账,且及时、确定的结算,以此降低结算总成本。全球各地的银行通过与 Ripple 合作来提供更好的跨境支付服务,并加入在价值网络基础上建立起来的、不断壮大的全球金融机构及做市商网络。	美国 加利福尼亚州	https://ripple.com/
43	BitPesa	金融服务	BitPesa 允许人们通过比特币来买卖非洲货币,交易结算直接通过非洲银行和移动资金账户来回进行。企业和交易商现在能够通过快速,低成本并且简单的支付方式在东非,中非和西非地区来回支付,消除了国际银行线路的压力和成本还有众多代理交易。	非洲 肯尼亚	https://www.bitpesa.co/
44	BitFury	区块链 基础设施	BitFury 由瓦罗维夫(Valery Vavilov)和瓦罗内森(Valery Nebesny)创立于 2011 年,是一家世界领先的比特币区块链基础设施供应商和交易处理公司,提供一系列的区块链软件及硬件产品,以支援商业和政府的区块链操作。该公司在过去几年持续有盈利,有总额超过 1 亿美元的收入。BitFury 已经在旧金山、华盛顿特区、香港、阿姆斯特丹和伦敦建立了管理办公室,同时还在冰岛和格鲁吉亚共和国建立了数据中心。	荷兰 阿姆斯特丹	http://bitfury.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
45	Blockstream	区块链基础设施	Blockstream 是一家专注于密码学货币创新的新成立的公司,联合创始人之一的艾森·希尔(Astin Hill)创建了曾开发出密码学隐私和匿名解决方案的零知识系统(Zero-Knowledge Systems),他也是电子现金(e-cash)早期的开发者。这家公司在2015年不仅推出了旗帜项目侧链(sidechain)的测试版,并宣布了第一个商业化产品 Liquid,目的是加快比特币交易所之间的资金传输时间。Blockstream 公司正在探索的另一个项目是闪电网络(Lightning Network),这个协议可以将小额的比特币交易带离区块链,这些交易可以更快并更经济地发生,更为重要的是,它仍实现了当前比特币网络无需受信的设计特性。	加拿大	https://blocks-tream.com/
46	Hyperledger	区块链基础设施	超级账本(hyperledger)是 Linux 基金会于2015年发起的推进区块链数字技术和交易验证的开源项目,加入成员包括:荷兰银行(ABN AMRO)、埃森哲(Accenture)等十几个不同利益体,目标是让成员共同合作,共建开放平台,满足来自多个不同行业各种用户案例,并简化业务流程。由于点对点网络的特性,分布式账本技术是完全共享、透明和去中心化的,故非常适合于在金融行业的应用,以及其他的例如制造、银行、保险、物联网等无数个其他行业。通过创建分布式账本的公开标准,实现虚拟和数字形式的价值交换,例如资产合约、能源交易、结婚证书、能够安全和高效低成本的进行追踪和交易。	美国马萨诸塞州	https://www.hyperledger.org/
47	Bloq	区块链基础设施	Bloq 将自身定位为“企业级区块链”服务,初始产品包括 BloqEnterprise, BloqSuite 和 BloqThink。Bloq 希望效仿红帽子的发展模式,即作为一个中间机构,处理好技术社区和想要利用这种开源操作系统的企业之间的矛盾,提供可行的解决方案。	美国伊利诺伊州	http://bloq.com/

48	BitGo	区块链基础设施	BitGo 是一家比特币安全平台,他们通过“多重签名比特币钱包”(“2 - of - 3 key” multi - signature)的方式,保障比特币持有者的资产安全。也就是说,用户在交易的时候,需要至少进行 2 ~ 3 次的确认。	美国加利福尼亚州	http://www.bitgo.com/
49	KnCMiner	区块链基础设施	总部位于瑞典斯德哥尔摩的 KnCMiner 公司由两大实力公司 ORSoC AB 和 Kenne-mar & Cole AB 联手打造设立。ORSoC 是一家业绩可考的专业嵌入式电子产品开发商,专注于 FPGA 及 ASIC 设计,拥有近 10 年综合设计服务及电子产品的开发经验,KnCMiner 因而组建了一支实力雄厚的硬件开发团队。	瑞典	http://www.kncminer.com/
50	Ledger	区块链基础设施	数字货币硬件钱包制造商 Ledger 是数字货币安全领域“技术领先”的公司之一,能为消费者和企业提供值得信赖的硬件。2015 年,Ledger 在种子轮融资中筹集到了 130 万欧元(约 150 万美元)。2016 年,Leger 凭借 TEE(可信执行环境)和 HSM(硬件安全模块)解决方案在 B2B 市场占据了自己的一席之地。	法国巴黎	https://www.ledger.co/
51	Trezor	区块链基础设施	Trezor 是第一个批量生产的比特币硬件钱包。硬件钱包不是普通的比特币客户端钱包,而是允许用户离线保存他们的比特币,但仍能够方便的发送比特币。	捷克	https://bitcointrezor.com/
52	KeepKey	区块链基础设施	KeepKey 是一家美国的数字货币硬件钱包制造公司,KeepKey 这款钱包可以让消费者离线存储比特币,从而避免比特币存储在计算机上或使用托管服务来存储比特币的种种安全问题。	美国华盛顿州	https://www.keepkey.com/
53	Tendermint	区块链基础设施	Tendermint 是一种开源的区块链套接字协议,能够促进分布式应用部署。Tendermint 区块链开发项目消除了区块链之前的复杂性,所以各种机构和自主程序员都能够轻松且高效地创建属于他们自己的区块链技术。	美国加利福尼亚州	http://tendermint.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
54	OpenShift	区块链基础设施	OpenShift 是红帽公司的第一个区块链项目,目标是帮助致力于该行业的金融企业以及进行该新兴科技相关的实验。通过 OpenShift 区块链,红帽公司的客户能够使用独立解决方案供应商(ISVs)提供的工具来创建托管的区块链应用,而且同时还能享受公司的管理支持服务。	美国	https://www.openshift.com/
55	Namecoin 域名币	区块链基础设施	域名币(Namecoin)是一个基于区块链技术的分布式域名系统,提供 . bit 等后缀的域名注册服务,具有安全和抗审查的特性。比特币矿工可以联合挖矿的形式,在挖比特币的同时一起挖域名币。	奥地利	https://namecoin.info/
56	Gem	区块链开发平台	Gem 拥有一个建立区块链应用层解决方案的核心平台,包括四个产品:Gem 身份、Gem 逻辑、Gem 数据和 Gem 网络。这四个组成部分合在一起可以建立一个完整的区块链生态系统和应用。	美国加利福尼亚州	https://gem.co/
57	Chain	区块链开发平台	Chain 创立于 2014 年,是一家业界知名的加州初创企业,他们帮助机构与企业定制部署区块链基础设施。团队前身是 Albumatic,一个照片共享的应用程序。	美国加利福尼亚州	https://chain.com/
58	Hedgy	区块链开发平台	Hedgy 公司的定位已经从最初的比特币和智能合约创业公司重塑为类似于 Chain 或者 Gem 的区块链应用程序开发平台。	美国加利福尼亚州	http://www.hedgy.co/
59	Peernova	区块链开发平台	据悉,Peernova 公司是由矿业公司 HighBitcoin 以及 CloudHashing 合并而来,2014 年 12 月,Peernova 融得了 860 万美元,并试图从挖矿公司转型到区块链应用公司。去中心化的应用(DApps),智能资产,智能合约以及电子货币软件应用程序将是 Peernova 主推的新方向。	美国加利福尼亚州	http://peernova.com/

60	Block Cypher	区块链 开发平台	成立于美国加州的 BlockCypher 提供一个加密货币应用程序可以很容易开发和扩展的平台。其中的一个关键部分是低延迟的 API 库和其他工具让实现区块链基础设施变得更加容易。	美国 加利福 利亚州	http:// www. blockcypher. com/
61	Stratumn	区块链 开发平台	Stratumn 的目的是将开发人员的在区块链上创建应用的想法变得更加容易实现,开发人员可以在 Stratumn 开发的平台上创建、部署和运行应用程序,并且这些应用程序还可以与比特币区块链之间进行连通,类似于 Heroku(一个支持多种编程语言的云平台即服务),区别是 Stratumn 平台针对区块链开发人员。	法国 巴黎	https:// stratumn. com/
62	Mijin	区块链 开发平台	Mijin 是一个区块链开发平台,其用户可以在点对点网络上轻松的创建私有区块链以及受许可的区块链。	日本	http:// mijin. io
63	Lisk	区块链 开发平台	Lisk 是一个致力于提供创建分布式应用程序(Dapps)的平台,这些 Dapps 将可能会颠覆整个应用市场,它们都是基于区块链技术。区块链技术赋予了这些 Dapps 数据安全性,零停机和防审查的优点。	德国	https:// lisk. io/
64	GetGems	社交通信	GetGems 是一个去中心化社交通信应用,其寻求通过发行于 Counterparty 上的原生币——GEMZ,使用户能够从平台的成长中获益,从而实现对其社交通信用户的激励。	以色列	http:// getgems. org/
65	ZapChain	社交通信	ZapChain 是一个比特币社交媒体平台。此外,ZapChain 还推出了新的数字化社区创建工具,用户可以使用比特币来激励社区,意味着发布内容,发起讨论或者出售产品或服务的用户,都可以使用到比特币微额支付。	美国 加利福 利亚州	https:// www. zapchain. com/

序号	项目名称	项目类型	项目简介	地区	官网链接
66	Steemit	社交通信	Steemit 是一个新型社交媒体平台,由区块链技术驱动,使用一种新的加密货币来奖励那些上传文章,图片和评论的用户。	美国 纽约州	https://steemit.com/
67	BitMessage 比特信	社交通信	比特信(Bitmessage)是一个去中心化通信软件,有棱镜杀手之美誉,它基于一个p2p的去中心化和无须第三方提供信用担保协议,不再需要根证书颁发机构。它使用了强大的认证,这意味着消息的发件人无法被欺骗。可以让你在匿名的情况下传输任何信息给接收者或者从一个发布者那里订阅信息。这一切都是建立在P2P网络上的,不存在一个中心服务器可以控制你的通信,窃听者也不能通过运行未经授权的程序监听你的消息。	美国	https://bitmessage.org
68	MaidSafe	数据存储	MaidSafe 致力于使用比特币区块链打造完全去中心化的互联网。	英国	http://maidsafe.net/
69	Storj	数据存储	Storj 基于区块链技术和点对点协议,为用户提供安全、私密、加密的云存储解决方案。	美国乔 治亚州	https://storj.io/
70	Sia	数据存储	Sia 最初的设计目的是:让云储存去中心化。当前,大多数数据由一个中心如亚马逊数据托管。一个单一的企业掌握着所有的数据,而且数据常常是不加密的。当前,把数据放在云中需要信任。你得相信亚马逊会保存你的数据并尊重你的隐私权。Sia 准备建立一套完全不同的系统来把数据放在云中。	全球 性组织	http://sia.tech/

71	Enigma	数据存储	Enigma 项目由 MIT 的研究生祖卡德 (Guy Zyskind) 研发, 并得到区块链创业家亚历克斯·彭特兰 (Oz Nathan) 以及 MIT (麻省理工学院) 教授阿勒·皮特兰德 (Alex Pentland) 的帮助, 用户们可以在市场上售卖大型计算与统计的加密数据, 同时不泄露数据的源地址。团队称项目会在不久的将来推出一个 beta 测试。	美国马萨诸塞州	http://enigma.media.mit.edu/
72	Elliptic	数据服务	从本质上来讲, 比特币网络交易是不透明的。尽管如此, 也有很多犯罪分子在进行国际汇款时会使用比特币洗钱。而凭借精良的工具和区块链探索器, Elliptic 就可以追溯部分交易的来源, 从而有可能为政府机构和执法部门跟踪交易的发起者。而消除欺诈交易和洗钱的企图, 可能会使比特币网络成为一个更可靠, 更安全的支付网络。	英国伦敦	https://www.elliptic.co/
73	Chainalysis	数据服务	Chainalysis 旨在通过跟踪链接到数字货币的数字身份来打击网络犯罪行为。该公司的软件能够立即检测可疑行为, 并为执法行动提供调查工具。	美国纽约州	https://www.chainalysis.com/
74	Scorechain	数据服务	Scorechain 公司总部位于卢森堡, 这是一家致力于为比特币公司和传统金融机构提供一整套帮助客户满足监管与合规要求的服务, 具体手段是通过商业智能和风险分析工具来明示区块链上的交易历史。	卢森堡	https://www.scorechain.com/
75	Skry	数据服务	Skry 原名 Coinalytics, 公司成立于 2014 年 4 月, 是一家提供实时数据情报服务的区块链数据公司。该公司通过区块链分析数据, 为比特币行业的客户, 比如支付处理公司、钱包提供商以及交易平台等进行风险评估。	美国加利福尼亚州	https://skry.tech/

序号	项目名称	项目类型	项目简介	地区	官网链接
76	TradeBlock	数据服务	TradeBlock(之前叫做“Genesis Block”)成立于2013年,由 Greg Schvey 和 Jeff Schvey 共同建立,提供全面的区块链交易数据分析。该公司希望简化用户访问比特币区块链的程序,包括比特币挖矿、比特币监管、比特币交易查询等。客户能够看到交易的执行,实时图表、订单以及其他来自 Tradeblock 国际资源的数据。这些信息剖析对于那些依靠数据获得竞争优势的企业来说非常重要。	美国 纽约州	https://tradeblock.com/
77	bitFlyer	数字资产交易	日本的数字资产交易所。	日本	https://bitflyer.jp
78	Coinsecure	数字资产交易	Coinsecure 是一家印度领先的比特币交易平台。它是印度唯一一家通过 ISO 认证的比特币企业,该公司提供了比特币钱包、交易所和商业服务。此外, Coinsecure 还拥有强大的开发者平台,并提供了一系列 API。该公司的总部设在德里,研究和开发部门则设在了班加罗尔。	印度	https://coinsecure.in/
79	Bitt	数字资产交易	Bitt 交易平台在数字金融方面是加勒比地区的一块奠基石。通过促进传统货币与数字货币之间的交易,Bitt 正在为最需要它的人们(即加勒比地区数百万无银行账户或者未能充分得到金融服务的人)建立一个交易成本极低的国际贸易和汇款平台。	加勒比地区	https://www.bitt.com/
80	SurBTC	数字资产交易	SurBTC 是一家智利比特币交易所。	智利	https://www.surbtc.com
81	Zebpay	数字资产交易	Zebpay 是一家印度的比特币钱包公司。	印度加 尔各答	https://www.zebpay.com

82	BitSquare	数字资产交易	BitSquare 是一个分布式交易所,支持虚拟货币和传统货币的交易。就像 Open Bazaar,它运行在 P2P 网络,这意味着没有中心服务器,不存储客户的自己和数据,黑客不能从它那里偷盗货币或信息。	西班牙	https://bitsquare.io/
83	Bitstamp	数字资产交易	BitStamp 是全球最大的比特币交易平台之一,总部在欧盟地区。它允许全世界的用户方便而安全的买卖比特币。	英国 伦敦	https://www.bitstamp.net/
84	Kraken	数字资产交易	Kraken 是一家总部位于旧金山的比特币交易所,目前, Kraken 已跻身美国最活跃的数字货币交易所阵列。	美国 加利福尼亚州	https://www.kraken.com/
85	itBit	数字资产交易	itBit 建立于2013年,目前是新加坡最被广泛认可的比特币交易所。2015年, itBit 获得了纽约州金融服务部颁发的信托公司章程,这让 itBit 成为了第一家获得此章程的比特币交易所,从而成为受美国银行法约束和监管的比特币公司。获得信托公司章程意味着 itBit 平台上的美元资金将被存在联邦存款保险公司担保的账户中。	新加坡	http://www.itbit.com/
86	Korbit	数字资产交易	Korbit 是一家韩国比特币交易平台,此外,还通过其产品 Korbit Pay 提供比特币钱包和商户处理服务,目前他们在交易平台以及钱包服务上拥有了约 30000 名用户,并且约有 400 家商家使用了 Korbit Pay 支付服务。	韩国	https://www.korbit.co.kr/
87	Coinplug	数字资产交易	Coinplug 是一家韩国比特币创业公司,始创于2013年。Coinplug 为韩国以及亚洲市场提供比特币交易所、钱包服务、okBitcard(比特币预付费卡)、双向比特币 ATM 机、支付处理服务。消费者和商家可以使用该公司的服务来接受比特币。	韩国	https://www.coinplug.com/

序号	项目名称	项目类型	项目简介	地区	官网链接
88	CEX. io	数字资产交易	CEX. io 为著名矿池 Ghash 推出的云算力交易平台,后转型为比特币交易平台,与矿机生产商 Bitfury、矿池 Ghash. io 关系密切。	英国伦敦	https://cex.io/
89	Coinbase	数字资产交易	Coinbase 是一个比特币钱包和交易所平台,商户可以通过 Coinbase 的服务接受比特币支付。自 2012 年建立以来,Coinbase 已经融资超过 1.05 亿美元。2014 年,Coinbase 成立美国首家正规比特币交易所,将为包括纽约、加州在内的 25 个州提供交易服务。这意味着 Coinbase 已获得美国多个州监管机构的合法执照。	美国加利福尼亚州	https://www.coinbase.com/
90	Gemini	数字资产交易	双子座(Gemini),由著名企业家和投资者卡梅伦和泰勒·文克莱沃斯双胞胎兄弟创立的比特币交易所,已获得了纽约金融服务部门(NYSDFS)的批准,可以为美国的客户提供比特币交易服务。	美国纽约州	https://gemini.com/
91	LaunchKey	物联网	LaunchKey 是一个去中心化的鉴权平台,为后密码时代以及物联网所设计。	美国内华达州	https://launchkey.com/
92	21 Inc.	物联网	21 公司出品的 21 比特币电脑,是第一台使用了原生硬件,且软件都是支持比特币协议的电脑。如果你是一个创业者或者开发人员,有了这个口袋大小的设备,你就可以通过命令行来使用比特币,实时地购买或销售数字商品和服务。	美国加利福尼亚州	https://21.co
93	IOTA	物联网	IOTA 是一个服务于物联网(IoT)生态系统的去中心化加密货币,它被建立于“Tangle 机制”之上而不是区块链之上。	挪威	http://www.iotatoken.com/

94	ADEPT	物联网	ADEPT 系统由 IBM 和三星联合打造,全称是“Autonomous Decentralized Peer – to – Peer Telemetry(去中心化的 p2p 自动遥测系统)”,它旨在为交易提供最优的安全保障。IBM 和三星希望这套系统可以让物联网里的各种设备自动运转,从理论上讲,家电的运转出故障时它们可以自动发送信号,并可以自动更新软件。甚至设备本身可以通过 ADEPT 来与周边的设备“沟通”,从而提高能源的利用效率。	美国	http://ibm.biz/devicedemocracy
95	Filament	物联网	Filament 是一个使用比特币区块链的去中心化的物联网软件堆栈,能够使公共分类总账上的设备持有独特身份。通过创建一个智能设备目录,Filament 的物联网设备可以进行安全沟通、执行智能合同以及发送小额交易。	美国内华达州	http://filament.com/
96	Tilepay 物付宝	物联网	Tilepay 物付宝,为现有的物联网行业提供一种人到机器或者机器到机器的支付解决方案。该公司开发了一个微支付平台,Tilepay 是一个去中心化的支付系统,它基于比特币的区块链,且能被下载并安装到一台个人电脑上、笔记本、平板或者手机上,所有物联网设计都会有一个独一无二的令牌,并用来通过区块链技术接收支付。Tilepay 还将建立一个物联网数据交易市场,使大家可以购买物联网中各种设备和传感器上的数据。并以 P2P 的方式保证数据和支付的安全传输。		http://www.tilepay.org/
97	Augur	预测市场	Augur 是建立在以太坊平台上的去中心化预测市场平台。利用 Augur ,任何人都可以为任何自己感兴趣的主体(比如美国大选谁会获胜)创建一个预测市场,并提供初始流动性,这是一个去中心化的过程。作为回报,该市场的创建者将从市场中获得一半的交易费用。许多因素使得 Augur 不同于传统的预测市场,但是最重要的区别是,Augur 是全球化去中心化的。世界各地的任何人都可以使用 Augur ,这将为 Augur 带来空前的流动性、交易量和传统的交易所不曾有过的多种视角和话题。	美国加利福尼亚州	https://www.augur.net/

序号	项目名称	项目类型	项目简介	地区	官网链接
98	Hivemind	预测市场	HiveMind 是一个基于区块链技术的去中心化预测市场,它被设计为比特币的一个侧链,它的理念是基于耶鲁统计学家 Paul Szore 提出的“Truthcoin”概念。Ver 将 HiveMind 描述为一个“利用群众智慧预测未来的令人难以置信的强大工具”。HiveMind 的目标之一就是创建一个平台,提供任何特定事件在未来发生的真实概率。	未知	http://bitcoinhive-mind.com/
99	Ethcore	智能合约	Ethcore 是一家区块链技术软件解决方案提供商,其软件方案释放了分布式技术的全部价值,使企业和组织都能从中发现新的价值和机遇。	英国伦敦	https://ethcore.io/
100	Rootstock	智能合约	Rootstock 是通过侧链的形式依附于比特币区块链的智能合约平台。	阿根廷布宜诺斯艾利斯	http://www.rootstock.io/
101	Counterparty	智能合约	Counterparty 是建立在比特币区块链之上,早期的 Bitcoin 2.0 项目之一。在本质上,它可以允许用户执行不同的金融应用,而不仅仅是比特币的 p2p 支付网络,并且它也受到比特币网络的保护。	美国纽约州	http://counterparty.io/
102	String	智能合约	String 是一家金融科技创业公司,他们为以太坊智能合约的开发者提供了一个去中心化的免许可的全球性金融环境。	美国加利福尼亚州	http://www.stringtechnology.com/

103	Colony	智能合约	Colony 是一个社会协作平台,可以减少管理分布在全球的员工的障碍。不同于经理指派任务,Colony 可以组成一个自治组织,集合项目员工的智力,消除等级管理制度,让员工投入自己的时间来获得权益,就像天使投资投入他们的资金一样简单。	英国伦敦	http://colony.io/
104	Ethereum	智能合约	Ethereum(以太坊)是一个平台和一种编程语言,使开发人员能够建立和发布下一代分布式应用。Ethereum 可以用来编程、分散、担保和交易任何事物:投票、域名、金融交易所、众筹、公司管理、合同和大部分的协议、知识产权,还有得益于硬件集成的智能资产。	全球性组织	https://www.ethereum.org/
105	Eris Industries	智能合约	Eris Industries 是一家成长非常快的区块链基础设施供应商,Eris 是一种企业级的区块链应用开发协议。Eris 已经获得 40 家全球大型金融机构的采用,包括普华永道(PWC)。Eris 开发的平台是唯一一个既能在亚马逊网络服务市场,也能在微软 Azure 上都可用的应用程序。	美国纽约州	https://erisindustries.com/
106	Counterparty 合约币	智能合约	Counterparty 是建立在比特币协议上的传输层,用来建立和使用去中心化的财务工具协议。简单来说,可以将 XCP 理解为很多“小的 BTC”即 XCP = “小的 BTC”,但是这些“小的 BTC”(XCP)不仅仅具有货币的交易功能,XCP 还具有资产发行(例如发行股票)、股息分配以及下注功能。	美国纽约州	http://counterparty.io/

附录3 区块链专业名词中英文对照表[\[60\]](#)

A

51% attacks 51% 攻击

account level(multiaccountstructure) 账户等级（多账户结构）

accounts 账户

addition operator 加法操作符

addr message 地址消息

Advanced Encryption Standard(AES) 高级加密标准(AES)

altchains 竞争币区块链

altcoins 竞争币

anonymity 匿名

assembling blocks into 将区块集合至

Asymmetric Cryptography 非对称加密

attacks 攻击

authentication path 认证路径

B

backing up 备份

balanced trees 平衡树

balances 余额

Base58 encoding Base58 编码

Base—64 representation Base—64表示

binary hash tree 二叉哈希树

BIP0038 encryption BIP0038 加密标准

Bitcoin 比特币

bitcoin addresses 比特币地址

bitcoin ledger 比特币账目

bitcoin network 比特币网络

Bitshares 比特股

Blake algorithm Blake 算法

Blockchain 区块链

block chain apps 区块链应用

block generation rate 出块速度

block hash 区块散列值

block header hash 区块头散列值

block headers 区块头

block height 区块高度

block templates 区块模板

blockchains 区块链

bloom filtersand 布鲁姆过滤器

BOINC open grid computingBOINC 开放式网格计算

broad casting to network 全网广播

broad casting transactions to 广播交易到

Byzantine Generals Problem 拜占庭将军问题

Byzantine Quorum Systems 拜占庭容错机制

C

centralized control 中心化控制

chaining transactions 交易链条

Chaumian blinding 盲签名技术

check Block function(Bitcoin Core Client) 区块检查功能 (Bitcoin Core 客户端)

checksum 校验和

child key derivation(CKD) function 子密钥导出(CKD)函数

child private keys 子私钥

coinbase 币基

coinbase rewards 币基奖励

coinbase transaction 币基交易

CoinDays 币天（币龄）

cold-storage wallets 冷钱包

ColoredCoin 彩色币

Collectively maintain 集体维护

compressed keys 压缩钥

compressed private keys 压缩格式私钥

compressed public keys 压缩格式公钥

computing power 算力

connections 连接

Consortium Blockchains 共同体区块链（联盟链）

Consensus 共识

constant 常数

constructing block headers 构造区块头部

converting compressed keys to 将压缩地址转换为

converting to bitcoin addresses 转换为比特币地址

counterparty protocol 合约方协议

Counterparty 合约币

CryptoCurrency 加密货币

CryptoCredits 加密信用

Cunning hamprime chains 坎宁安素数链

currency creation 货币创造

D

data structure 数据结构

decentralized 去中心化

decentralized consensus 去中心化共识

decoding Base58Check to/from hexBase58Check 编码与16进制的相互转换

decoding to hex 解码为16进制

deflationary money 通缩货币

delegated proof of stake 股份授权证明

demurrage currency 滞期费

denial of service attack 拒绝服务攻击

deterministic wallets 确定性钱包

difficulty bits 难度位

difficulty retargeting 难度调整

difficulty targets 难度目标

digital signature 数字签名

digitalnotary services 数字公证服务

Distributed Ledger 分布式账本

domain name service(DNS) 域名服务(DNS)

double-spend attack 双重支付攻击

dual-purpose 双重目标

dual-purposemining 双重目的挖矿

dust rule 尘额规则

E

electricity cost 电力成本

electricity cost and target difficulty 电力消耗与目标难度

Electrum wallet Electrum 钱包

Elements 元素链

Ethereum 以太坊

ellipticcurve multiplication 椭圆曲线乘法

encoding/decoding from Base58Check 依据Base58Check 编码/解码

encrypted 加密

encryption algorithm 加密算法

encrypted private keys 加密私钥

extended key 扩展密钥

extra nonce solutions 添加额外随机数的方式

F

fees 手续费

field programmable gate array(FPGA) 现场可编程门阵列(FPGA)

fork attack 分叉攻击

forks 分叉

full nodes 完整节点

G

generating 生成

generation transactions 生成交易

generator point 生成点

genesis block 创世块

genesis block 创世区块

GetBlock Template(GBT)mining protocolGBT 挖矿协议

GetWork(GWK) mining protocol GWK 挖矿协议

graphical processing units(GPUs) 图形处理单元(GPUs)

H

hackers 黑客

hardware wallets 硬件钱包

Hash 哈希，又称散列

HashCash 哈希现金

Hashed Timelock Contract 哈希时间锁定合约HTLC

hashing powerand 哈希算力

HD walletHD 钱包

header hash 头部散列值

Hierarchy deterministic 分层确定的

Hyperledger 超级账本

I

identifiers 标识符

immutability of blockchai 区块链不可更改性

in block header 在区块的头部

independent verificatio 独立验证

I owe you 借据 (IOU)

K

key formats 密钥格式

L

Level DB database(Google)LevelDB 数据库(Google)

light weight 轻量级

Lightning Network 闪电网络

lock time 锁定时间

lock time 锁定时间

locking scripts 锁定脚本

M

managed pools 托管池

Mastercoin 万事达币

memorypool 内存池

merkle tree 默克尔树

merged mining 合并挖矿

metachains 附生区块链

Micro-Payments Channel 微支付通道

mining 挖矿

mining blocks successfully 成功挖出区块

mining pools 矿池

mining rigs 矿机

modifying private key formats 修改密钥格式

monetary parameter alternatives 货币参数替代物

Moore's Law 摩尔定律

multi account structure 多重账户结构

multi-signature address 多重签名地址

multi-signature addresses 多重签名地址

multi-signature scripts 多重签名脚本

multi-signature account 多重签名账户

N

Namecoin 域名币

nodes 节点

nonce 随机数

noncurrency 非货币

nondeterministic wallets 非确定性的

O

on full nodes 在全节点上

on new nodes 在新节点上

on SPV nodes 在SPV 节点

on the bitcoin network 在比特币网络中

OP_RETURN operatorOP_RETURN 操作符

OpenSSL cryptographiclibraryOpenSSL 密码库

orphan block 孤块

outputs 输出

P

P2P Pool 点对点挖矿的矿池

parent blocks 父区块

peer-to-peer networks P2P 网络

physical bitcoin storage 比特币物理存储

Practical Byzantine Fault Tolerance 改进型实用拜占庭容错机制（简称PBFT）

Premine 预挖

priority of transactions 交易优先级

Private Blockchain 私有区块链

Proof of existence 存在性证明

proof of stake 权益证明

proof of work 工作量证明

propagating transactions on 交易广播

protein folding algorithms 蛋白质折叠算法

Public Blockchain 公共区块链（公有链）

public child key derivation 公钥子钥派生

public child key derivation 导出公有子密钥

publickeys 公钥

public key derivation 公钥推导

purpose level(multiaccount structure)目标层（多帐户结构）

Python ECDSA library PythonECDSA 库

R

random 随机

retargeting 切换目标

Reliable Database 可靠数据库

Reusable Proofs of Work 可复用的工作量验证

Revocable Sequence Maturity Contract 序列到期可撤销合约RSMC

RIPEMD160RIPEMD160算法

Ripple Consensus Protocol 瑞波共识协议

risk balancing 适度安保

risk diversifying 分散风险

root of trust 可信根

root seeds 根种子

S

satoshis 聪

scriptcons truction 脚本构建

script language for 脚本语言

Script Language 脚本语言

scripts 脚本

script algorithmscript 算法

script-N algorithmscript-N 算法

Secure Hash Algorithm(SHA)SHA 哈希算法

Secure Multi-party Computation 多方安全计算

seed nodes 种子节点

seeded 种子

seeded wallets 种子钱包

Segregated Witness 隔离见证

shopping carts public keys 购物车公钥

simplified payment verification (SPV)简易支付验证 (SPV)

sidechains 侧链

Skein algorithmSkein 算法

smart contracts 智能合约

smart pool 机枪池

solo miners 独立矿工

solo mining 单机挖矿

stateless verification of transactions 交易状态验证

statelessness 无状态

Stellar Consensus Protocol(SCP)恒星共识 (SCP)

storage 存储

Stratum(STM)mining protocolStratum 挖矿协议

syncing the blockchain 同步区块链

system security 系统安全

T

taking off blockchain 从区块链中删除

testnet 比特币测试网络

timeline 时间轴

timestamp 时间戳

token system 代币系统

transaction fees 矿工费

transaction fees 交易费

transaction pools 交易池

transaction validation 交易验证

transactions independent verification 独立验证交易

tree structure 树结构

Trezor walletTrezor 钱包

Turing Complete 图灵完备

trust in a third party 可信第三方

tx message tx 消息

Type-0 nondeterministic wallet 原始随机钱包

U

uncompressed keys 解密钥

unconfirmed transactions 未确认交易

user security 用户安全性

UTXO 未花费的输出

UTXO poolUTXO 池

UTXO setUTXO 集合

V

validating new blocks 验证新区块

validation 验证条件

validation(transaction) 校验(交易)

vanity addresses 个性地址

vanity-miners 个性地址挖掘程序

verification 验证

verification criteria 验证条件

version message 版本信息

W

Wallet Import Format(WIF)钱包导入格式

wallets 钱包

[\[60\]](#) 巴比特翻译小组整理。

图书在版编目 (CIP) 数据

区块链:从数字货币到信用社会 / 长铗等著.—北京: 中信出版社, 2016.7

ISBN 978-7-5086-6344-9

I. ①区... II. ①长... III. ①电子商务—支付方式—研究 IV. ①F713.36

中国版本图书馆CIP数据核字 (2016) 第126195号

区块链:从数字货币到信用社会

著者: 长铗 韩锋 等

策划推广: 中信出版社 (China CITIC Press)

出版发行: 中信出版集团股份有限公司

(北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029)

(CITIC Publishing Group)

电子书排版: 张明霞

中信出版社官网: <http://www.citicpub.com/>

官方微博: <http://weibo.com/citicpub>

更多好书, 尽在中信书院

中信书院: App下载地址<https://book.yunpub.cn/> (中信官方数字阅读平台)

微信号: 中信书院

BLOCKCHAIN: RESHAPE THE ECONOMY AND THE WORLD

区块链

重塑经济与世界

徐明星 刘勇 段新星 郭大治 - 著

一本书让你读懂区块链

高盛、IBM、花旗银行、摩根士丹利、纳斯达克、德勤等各类巨头趋之若鹜

让苹果、谷歌、脸书感受到威胁的区块链到底是什么

去中心化、分布式账本、点对点传输……
将从根本上改变我们的生活

区块链：重塑经济与世界

徐明星 刘勇 段新星 郭大治 著

中信出版集团 · CHINACITICPRESS · 北京

目 录

[前言](#)

[第一章 探寻区块链的源头——“重回拜占庭”](#)

[拜占庭将军的难题](#)

[古老的“拜占庭将军问题”](#)

[“拜占庭将军问题”在通信领域的意义](#)

[用算法解决难题——区块链技术的雏形](#)

[区块链之父——中本聪](#)

[神秘的中本聪，神秘的论文](#)

[波动的价格，轰动的交易](#)

[传输价值的代币](#)

[区块链到底是什么](#)

[比特币与区块链是父与子关系吗](#)

[层出不穷的其他数字货币](#)

[区块链的实际应用](#)

[区块链的颠覆特点](#)

[第二章 区块链——颠覆世界的力量](#)

[颠覆的核心——去中心化](#)

[去中心化——“鸟群智慧”的一角](#)

[为什么去中心化一定会成功](#)

[区块链的去中心化技术意味着什么](#)

[区块链将构建完美的契约世界](#)

[智能合约赋予物联网“思考的力量”](#)

[从智能合约到智能资产](#)

[有执行力的合约](#)

[区块链未来应用蓝图](#)

[为什么区块链会率先颠覆金融领域](#)

[区块链技术将成为下一代数据库架构](#)

[区块链将如何颠覆我们的生活](#)

[各国政府的态度——从比特币到区块链](#)

[区块链1.0：游走在法律边缘的比特币](#)

[后比特币的2.0时代](#)

[各国政府对比特币的监管](#)

[区块链技术可以被用于创造更多的集中式数字货币](#)
[商业银行基于区块链的应用领域](#)
[第三章 区块链率先敲开金融的大门](#)
[从贝壳到数字货币](#)
[货币的演变](#)
[央行与数字货币——不可或缺的区块链](#)
[Fintech（金融科技）创新最前沿——区块链技术](#)
[金融拥抱区块链](#)
[支付汇款——变革的前夜](#)
[区块链将重构股权清算结算](#)
[股权众筹——基于区块链技术的畅想](#)
[票据业务——依托区块链平台的改造](#)
[金融基础设施革命](#)
[区块链对审计行业的颠覆](#)
[资产确权——区块链让难题变得如此简单](#)
[智能合约——不可思议的区块链技术](#)
[第四章 链接万物的区块链](#)
[这个房子属于我吗——区块链给你证明](#)
[如何继承父母房产](#)
[洪都拉斯的拆迁纠纷](#)
[传统认证系统的缺点](#)
[区块链技术可以解决公证和认证的问题](#)
[从Stampery到Chronicled，区块链公证业务的实践](#)
[我还是我吗——在区块链上很简单](#)
[如何证明“我妈是我妈”](#)
[分布式智能身份认证系统](#)
[区块链上享受结婚证明](#)
[DAOs（去中心化自治组织）](#)
[即将诞生的区块链总统](#)
[BitNation（比特国）](#)
[区块链上的DAOs](#)
[区块链让物联网真正链接万物](#)
[更安全的物流和供应链](#)
[智能物联网](#)
[聚沙成塔的分布式云存储](#)
[分布式云存储](#)

[其他区块链相关服务](#)

[自由交易：下一个阿里巴巴](#)

[21 Inc：共享经济的延伸](#)

[第五章 区块链应用的全球进展](#)

[BitPay融资3000万美元，估值达1.6亿美元](#)

[Coinbase正式完成7500万美元C轮融资](#)

[超越Coinbase，初创比特币公司21 Inc获1.16亿美元巨额融资](#)

[智能合约平台Symbiont获700万美元融资](#)

[比特币区块链应用公司PeerNova融资860万美元](#)

[智能合约交易平台Mirror获A轮880万美元融资](#)

[区块链公司Chain获3000万美元融资](#)

[Chainalysis募集160万美元的资金，与欧洲刑警组织签署网络犯罪协议](#)

[当黄金遇见区块链技术：BitGold获350万美元A轮融资](#)

[Align Commerce获1250万美元A轮融资](#)

[比特币公司Blockstream斩获A轮5500万美元融资](#)

[区块链创业公司Gem完成710万美元A轮融资](#)

[去中心化淘宝OpenBazaar获得100万美元种子投资](#)

[高盛、IBM追投，区块链公司DAH融资6000万美元](#)

[用区块链技术买东西？Colu获250万美元融资](#)

[附录 区块链技术名词与核心原理](#)

[参考文献](#)

前言

2008年，一个神秘的人物，直至今日只闻其名未见其人的“中本聪”通过一篇未在任何学术期刊上公开发表的神秘论文，把比特币带到这个世界。诞生于虚拟世界的比特币代表了人类对于数学算法的一种共识，基于这种共识机制，即使没有任何政府信用背书，比特币仍然获得了世人的认可，不论是从最初几十个比特币换取一份比萨，还是2013年12月1日，比特币的单价超越一盎司黄金的价格，比特币都在向世人展示其作为价值尺度的一面。尽管比特币价格的暴涨暴跌使其减弱了在更大范围内作为货币应用的可能，但比特币向世人展示了一种不需要中介却可以实现价值传递的可能性。这种可能性就是区块链。

正如梅兰妮·斯万（Melanie Swan）指出的那样，比特币和区块链包括三个层次的内容：区块链底层技术、协议和加密数字货币。区块链技术是点对点通信技术和加密技术的结合，基于区块链技术生成的区块链本质上是一个去中心化的分布式账本数据库；在这个数据库的基础上可以开发出数目繁多的应用，这些应用通过协议层面建立共识机制实现各种功能；最后应用层面，客户可以实现无需中间权威仲裁的点对点的交互，当然包括比特币。有人用“组织形式上的去中心化和逻辑上实现完美一致性的技术”来形容区块链技术，也有人用“下一代全球信用认证和价值互联网的基础协议之一”来阐述区块链的特点，总体而言区块链技术的应用主要包括以下内容。

一是金融产品创新。由于金融产品基础结构的主要内容就是关于参与各方权利义务的约定，货币、债券、股权等各类金融产品都可以通过协议层建立共识机制形成与传统金融产品类别相对应的创新金融产品。由于区块链形成了可以独立存在的共识机制，因此区块链技术具有自动执行协议的功能，人们将此类协议归类为智能合约。智能合约实施的基础是共识机制而非中心化的验证，使得智能合约的执行成本降到最低、执行效率大大提升。基于智能合约运行的创新金融产品具有高透明度、高安全性、高效率的显著特征。基于上述优势，区块链技术对金融行业的改变将是颠覆性的，现有金融体系中的一些角色将不再需要，金融中介的职能也将发生深刻变化。

二是金融基础设施的变革。区块链本身就是一个数据库，基于点对点的通信技术和加密技术使数据库的组织形式更具开放性和可追溯性。在区块链技术的基础上，每个数据节点都可以参与验证账本内容的真实性和完整性，相当于通过提高系统的可追责性降低系统的信任风险。这一特性使得区块链在征信、审计、资产确权等方面具有显著的优势，从而间接提高金融体系的运行效率。

三是智能物联网。由于区块链形成了独立运行的共识机制，区块链技术可以应用于物联网的数据处理和系统维护领域。比如已经有机机构提出要使用区块链技术管理上百亿个物联网设备的身份、支付和维护任务。利用区块链技术，物联网设备生产商能够极大地延长产品的生命周期和降低物联网维护的成本。

四是共享经济的技术基础。区块链去中心化的共识机制使得计算服务的应用范围大大延伸。尽管电子支付技术的发展大大降低了支付的成本，但现有支付业务模式下极小金额的支付比如低于0.01元的支付成本仍然非常高。有公司正在开发一种基于区块链的微支付技术，为每个人的电脑利用闲置计算能力从事挖矿、存储等工作提供计量工具。这种计量服务正是多种共享经济的前提，将大大拓宽共享经济的深度和广度。

综上所述，区块链技术的主要优势在于基于分布式网络形成的共识机制，分布式网络使得基于区块链的应用具有明显的开放性和可拓展性，这样会使一些商业模式的门槛可以降低得很低，甚至产生全新的商业模式；共识机制的独立存在使合约的执行成本降到最低，执行效率大大提升，计算服务的范围也大大提升。

全球正在掀起一股区块链的热潮。来自学术界和科技界的各种力量投身区块链的开发和创业大潮之中，也诞生了一批非常有创新意识的创业公司，成为Fintech（金融科技）中的一股重要力量；到2015年底，已经有超过20家全球顶级的金融机构、风险基金高调宣布参与各种区块链应用开发项目。当然，我们也必须要清醒地看到，区块链技术的发展不论在国际还是在国内都尚处在早期阶段，各种技术方案和商业模式等都需要进一步地探索和实践。特别是在我国，区块链作为一个全新的概念和理论，人们的认知、研究和实践刚刚起步，要想在这一领域积累优势，引领世界，还需要足够的重视，更多的投入，需要理论研究者、网络技术者、金融从业者，以及政府监管部门的积极投入和良性互动。正是在这样的大背景下，《区块链：重构经济与世界》的出版正好填补了国内关于区块链技术特点和应用分析的空白，希望此书的出版为我国区块链技术的开发应用提供一定的参考和借鉴。

第一章

探寻区块链的源头

——“重回拜占庭”

每一个时代都有自己值得骄傲的技术，无论是晶体管、激光、互联网，还是载人航天飞机。近10年中，金融网络领域最具颠覆性、最闪耀的技术发明莫过于区块链。无论是与数字货币一道横空出世，继续发力衍生出智能合约，还是可预见的未来，不断重塑整个金融世界，都使它的夺目光芒无法掩盖。然而究其源头，我们不得不追溯到“拜占庭将军问题”和“双花问题”。后者比较简单，即如何杜绝非实体货币的再次被使用，或者是双重支付（只要引入盖时间戳的电子签名就能解决）。而前者，“拜占庭将军问题”则看起来费解且扑朔迷离，但我们又不能回避，因为它是整个区块链技术核心思想的真正根源，也直接决定了区块链技术的种种与众不同的颠覆性特质。

在某种程度上，问题比答案更重要。很难想象：如果没有“拜占庭将军问题”，没有它揭示出在人类散兵游勇的状态下，永恒的“共识”困境，那么对于这种困境的反思和探索便无法成为可能，逃离困境到达光明之地也无法成为可能。所以在我们向伟大的“答案”——区块链致以敬意之时，请不要忘记它的源头，不要忘记拜占庭。

拜占庭将军的难题

古老的“拜占庭将军问题”

让人生，让人死，让人痴迷，让人疯狂。

这就是传说中繁华与没落，绝望与救赎并存的东罗马帝国首都，拜占庭。

在2013年获得计算机科学领域最高奖项图灵奖的31年前，1972年，莱斯利·兰伯特（Leslie Lamport）搬到湾区。此时，他仍然是一个寂寂无闻的美国小伙。他充当Compass（马萨诸塞州计算机合伙人公司）西海岸计划前哨基地的先锋，不幸的是，这个分支机构最终未能落实。在长达5年的时间里，他曾是Compass总部派驻加州的唯一员工。最后，他却收到撤回东海岸的指令。于是，他决定加入斯坦福国际研究院（SRI）。在那段岁月里，SRI有一个项目，要在美国航空航天局建立容错型航电计算机系统。考虑到系统的工作性质，故障是不允许发生的。这段经历孕育了两篇旨在解决一种特殊故障的论文，由兰伯特和SRI同事马歇尔·皮斯（Marshall Pies）及罗伯特·肖斯塔克（Robert Shostak）合作完成。用计算学术语说，普通故障可能会导致信息丢失或进程停止，但系统不会遭到破坏，因为这种普通故障属于一出错就会停下来的故障类型，剩下的备份的、正常的部分照样可以运转，发挥作用。就像战场上的士兵，他们一旦受伤或阵亡就停止战斗，但并不妨碍他人继续作战。

然而一旦发生“拜占庭故障”，就会非常麻烦，因为它们不会停下来，还会继续运转，并且给出错误讯息。就像战争中有人成了叛徒，会继续假传军情，惑乱人心。当时为了解决这个问题，常常使用的技术被称为“三重模块冗余”：也就是说使用三台计算机进行万一出错的备份工作，三台独立的计算机按照少数服从多数的原则“投票”。这样，即使其中一台机器提供了错误结果，其他两台仍然会提供正确答案。但是为了证明这种方法的有效性，必须拿出证据。而在编写证据的过程中，研究人员遇到了一个问题：“错误”计算机可能给其他两台计算机发送互不相同的错误值，而后者却不知道。这就需要使用第四台计算机来应对这个故障。

兰伯特说：“如果你使用数字签名，就可以用三台机器达成目的，因为如果‘坏了’的计算机向一台计算机发送了带签名的错误值，并向另一台发送了不同的带签名错误值，另外两台计算机就能够交换消息，以检查究竟发生了什么情况，因为两个不同的值都是签名发送的。”兰伯特还听吉姆·格雷谈论过另一个性质大体相同的问题，人们称之为“中国将军问题”。这引起了兰伯特有关司令将军和叛徒将军的联想，于是他将这个问题及其解决方案命名为“拜占庭将军问

题”。

“我记得，与我的朋友怀特·迪菲（White Duffy）坐在伯克利的一间咖啡馆里，当时他描述了一个构建数字签名的问题。”兰伯特回忆说，“他说：‘如果能办到的话，会非常有用。’我说：‘这听起来并不很困难。’于是在一张餐巾纸上，我为他勾画出了第一种数字签名算法。虽然当时并不很实用，但目前已经变得切实可行。”只可惜那张餐巾纸已经消逝在时间的流沙中。在后来1982年正式出版的拜占庭将军论文的序言中，他这样写道：

“我一直觉得正是因为通过用一组围坐在圆桌旁的哲学家来表述，Dijkstra（迪克斯塔）的‘哲学家就餐问题’才变得如此让人关注（比如在理论界，它可能比‘读者/作者’问题都引人注目，尽管读者/作者问题可能更具实际意义）。我认为Reaching Agreement in the Presence of Faults（达成共识的缺陷）中所描述的问题十分重要，值得计算机科学家们去关注。‘哲学家就餐问题’使我认识到，把问题以讲故事的形式表达出来更能引起人们的关注。在分布式计算领域有一个被称作‘中国将军问题’的问题。在这个问题中，两个将军必须在进攻还是撤退上达成一致，但是相互只能通过信使传送消息，而且这个信使可能永远都无法到达。我借用了这里的将军的叫法，并把它扩展成一组将军，同时这些将军中有些是叛徒，他们需要达成一致的决策。同时我想给这些将军赋予一个国家，同时不能得罪任何读者。那时候，阿尔巴尼亚还是一个完全封闭的国家，我觉得应该不会有阿尔巴尼亚人看到这篇文章，所以最初的时候这篇论文题目实际是The Albanian Generals Problem（阿尔巴尼亚将军问题）。但是Jack Goldberg（杰克·古登博格）后来提醒我，在这个世界上除了阿尔巴尼亚之外还有很多阿尔巴尼亚移民，所以建议我换个名字。于是就想到了这一更合适的叫法——Byzantine generals（拜占庭将军）。 ”

写这篇论文的最主要目的是将拜占庭将军这个叫法用在这个问题上。基本的算法文章在1980年的论文中就已经出现了。

起源：拜占庭位于现在土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了防御敌人每个军队都分隔很远，将军与将军之间只能靠信差传消息。在战争时期，拜占庭军队内所有将军和副官必须达成一致共识，决定是否有赢的机会才去攻打敌人的阵营。但是，军队可能有叛徒和敌军间谍，左右将军们的决定，扰乱军队整体的秩序。在达成共识的过程中，有些信息，往往并不代表大多数人的意见。这时候，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，就是“拜占庭将军问题”。

两军问题：军队与军队之间分隔很远，传递信息的信差可能在途中阵亡，或因军队距离不能在得到消息后即时回复，发送方也无法确认消息确实丢失的情形，导致不可能达到一致性。在分布式计算上，试图在异步系统和不可靠的通道上达到一致性是不可能的。因此对一致性的

研究一般假设信道是可靠的，或非异步系统上运行。[\[1\]](#)

“拜占庭将军问题”在通信领域的意义

“拜占庭将军问题”并非如传说中那样，源于公元5世纪的东罗马战场，而是产生于1982年一位美国计算机科学家的头脑当中。因此，我们不会使用任何1982年之前的案例来描述这个问题在古老年代的意义，因为再往前追溯，它并未真正、严肃地被提出并加以审视。

在原始的战争年代，将军与将军、将军与下属间只能采用原始的方式——“出行靠走，通讯靠吼”的口头传输。这对应兰伯特论文提出算法中的第一部分的口头消息算法，简称OM(m)算法。这种情形，真伪很难辨别，只有当叛徒的总数不超过将军总数的 $\frac{1}{3}$ ，成为一个特殊的“拜占庭容错系统”时，才能在很大的消息验证代价后，实现最终的一致行动。这个结果非常令人惊讶，如果将军们只能发送口头消息，除非超过 $\frac{2}{3}$ 的将军是忠诚的，否则该问题无解。尤其是，如果只有三个将军，其中一个是叛变者，那么此时无解。但这样的错误，这样的有意、无意的“叛徒”却可能经常出现。无论是我们把“叛变的将军”替换成以下哪种，该问题都成立。

- 一个出故障的，向其他计算机不停发出不同错误信息的服务器；
- 一份为获取暴利而做出来的金融票据；
- 一份失效的医疗纠纷合同；
- 一份含混不清的保单；
- 一个可以发出消息，做出行动的错误信息节点。

而这里，每一个错误节点可以做任意事情：不响应；发送错误信息；对不同节点发送不同决定；不同错误节点联合起来攻击其他节点等。没准会出现比这更严重、更荒谬的错误。

如果说“叛变的拜占庭将军”是我们社会中各种类型的信息节点的隐喻，那么“拜占庭将军问题”所描述的情景，这样一个进攻 / 撤退命令极难验证真伪的中世纪战场，则无疑是我们当今越发缺乏中心化的、难以判别信息与产生信任的社会的极度悲观的隐喻。

用算法解决难题——区块链技术的雏形

构造出一个完美的、可以解决问题的“拜占庭容错系统”是一个不小的挑战。而且构造出来以后，其是否真的有效，能否经得起时间的考验与各方的质疑，这些都关乎着这个系统未来的命运与其创造群体的声誉。

2008年冬季，美国MIT（麻省理工学院）的密码学及密码学政策战略的邮件讨论组中，一位澳大利亚的企业家James A. Donald（詹姆斯·A. 唐纳德）就对一位声称构造出了一个点对点的、不需要第三方权威认证的e-cash（电子现金）支付系统提出了质疑。而他的理由就是：对方设计的P2P系统不能够解决“拜占庭将军问题”。

在邮件中他挑剔地说道：“我们的确真的非常非常需要这个系统，但我所担忧的并不是信任的问题，而是如何获取一个全局共享的图景，借由此点而获取一致性的问题。每个人都知道X，这并不足够。我们需要让每个人都知道‘每个人都知道X’。而每个人都知道‘每个人都知道X’就是‘拜占庭将军问题’中，分布式的数据处理最难解决的问题。尤其是当X是非常庞大的数据时……”言下之意，他并不清楚或不确信这个去中心化的系统，如何解决拜占庭将军的难题。

仅仅在一天之后，他就收到了原作者的回复，一封简洁、优雅的邮件解释了在这个系统中，破解“拜占庭将军问题”的算法。^[2]

“工作量证明链”（proof-of-work chain）正是我解决“拜占庭将军问题”的方案。我将在那个语境中对它进行重新表述。

一群拜占庭将军，人手一台电脑想用字符串模式匹配的方法，暴力破解国王的Wi-Fi密码，当然他们已经事先获取了组成密码的字符串的长度。一旦他们开始模拟网络发送数据包，他们必须在一个限定的时间内完成破解工作，并清除服务器和电脑上的记录，否则他们就会被发现，那就麻烦了。只有当绝大多数将军在同一时间发起攻击和破解，这样才能有足够的CPU（中央处理器）和计算能力在短时间内完成破解工作。

他们并不特别在乎什么时候开始攻击，只要他们全部同意就好。一开始的时候，大家决定这样搞：任何人觉得时机到了都可以宣布一个攻击时刻。而且，不论是什么时候，只要是第一个被听到的攻击时刻，就将被确定为官方的攻击时刻。这样的话问题又来了，因为网络传达有延迟和干扰，如果有两个将军差不多同一时间公布了两个不同的攻击时刻，那么有的人会最先听到其中一个将军发布的攻击时刻，而又有些人则会最先听到另外一个将军发布的攻击时刻。

他们使用一个“工作量证明链”来解决这个问题。当每个将军接收到任何表达形式的第一个攻击时刻时，他都会设置他的计算机来求解一个极其困难的“工作量证明”问题，对这个问题的解答是一个哈希（Hash）散列，里面也将包含着这次的攻击时刻。由于这个“工作量证明”问题，非常难解，一般而言，就算所有人收到这个问题后同时求解，也至少需要10分钟才能产生解答。一旦一个将军解出了“工作量证明”，他将会把这个算出来的“工作量证明”向

整个网络进行传播，每一个接收到的人，将在他们当前正在做的“工作量证明”计算的散列中附上刚刚被求解出来的那个工作量证明。如果任何人正在计算他收到的其他的一个不同的攻击时刻，他们将会转向新的更新后的“工作量证明”计算当中，因为他现在的“工作量证明链”更长了。

两个小时后，将有一个攻击时刻被散列在一个有12个“工作量证明”的链中。每个将军只要通过验证（这条工作链的）计算难度，就能估算出平均每小时有多少CPU算力耗费在这上面，也就会知道：这一定是在分配的时间段内，绝大多数将军的计算机共同协作才能生成的结果。如果“工作量证明链”中展示出来的算力足够强大，可以破解国王的Wi-Fi密码，那么他们就可以在一致同意的时间内安全地展开攻击。

同步、分布式数据库和一个一致的、全局性的视野的问题如何解决？“工作量证明链”就是答案。

我们可以看到这封邮件解决了下面几个问题：

（1）引入一个困难的、需要10分钟求解的工作量计算，限制了网络中每个时刻中被提出的进攻时刻数目。

（2）将所有求解出的“工作量证明”都逐一加入，形成一个越来越长的链条，一个记录着所有“参与着攻击时刻哈希计算的将军、计算的‘工作量证明’、关于‘工作量证明’的计算的总体名录”。

（3）基于这条长链得出安全的进攻时刻的答案。

最后，请各位读者注意这封解释邮件头上的内容：

日期：2008年11月14日06:56:55 (GMT+8)

邮件作者的签名：Satoshi Nakamoto

区块链之父——中本聪

神秘的中本聪，神秘的论文

上一节中，用“国王的Wi-Fi”解释“拜占庭将军·难题”算法的邮件作者，名叫Satoshi Makamoto，如果你对这个英文名字感到陌生，不妨看看其他几个译名：

日语翻译：中本哲史；

汉语翻译：中本聪。

比特币圈内的人一定都知道他的大名：一个匿名者、一个爱收集火车模型的天才黑客。人们关注他的理由还有很多：不仅因为他发明了比特币，还因为传言他拥有一笔类似尼伯龙根宝藏一样的海量比特币财富，以及其他诸多不为人所知的内容。然而，所有寻找中本聪的努力都以：

- 相同的方式开始（我们找到了！）；
- 相同的方式高潮（看似可靠，但并不有力的证据引发坊间的热议）；
- 相同的方式落幕（被怀疑或证明不是）。

无论是《新闻周刊》《纽约时报》，还是《连线》杂志近来出现的寻找中本聪的数次“乌龙”，让人们甚至开始计数，“这是第12次还是第13次发现‘真正’的中本聪了？”

他的最近一次露面是沉寂多年后的又一封声明：2015年12月在Linux基金会的比特币开发者群组中：

邮件标题：“Not this again.”（这次你们仍然没猜对）

正文：“I am not Craig Wright. We are all Satoshi.”（我不是克雷格·赖特，我们都是中本聪）

这次媒体炒作源于2015年12月8日，《连线》刊文认为克雷格·斯蒂文·赖特（Craig Steven Wright）即中本聪，并列举了部分掌握的“可靠”证据，包括猜测在一段可能要发言的视频中所要说的话和内容。之后数小时，澳洲警方突袭并搜查了他的家，但警方称此次搜查是和税务相关，与比特币没有联系。《卫报》援引路透社记者称，赖特的办公室也遭到了搜查。

然而这次搜查之后，中本聪的声明并没有得到开发者群体的广泛关注。事实上，自2014年9月起，就有确定的网络证据显示：部分中本聪的邮箱账户已经“有意无意”地被盗。甚至，盗取者本人对此也供认不讳，并颇为得意地提醒：中本聪先生保密工作没有做够，为安全起见请赶紧逃离，以防被抓捕。在揶揄的同时，仍然不忘记来一句Thank you for inventing Bitcoin（多谢你发明了比特币）。

下图是2014年中本聪的邮箱因长期荒废等原因被黑客盗用，从此更难有任何可信的渠道证明任何发表声明的是其本人。

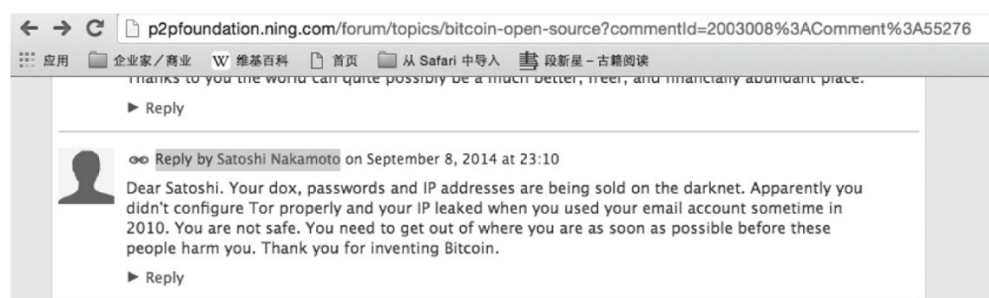


图1-1 中本聪邮箱账户被盗，并用中本聪账户发表声明

资料来源：<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?id=2003008%3ATopic%3A9402&page=4#comments>

这看起来似乎是一件非常滑稽的事，多么地矛盾！中本聪的密码学造诣十分精湛，许多曾经被认为是冗余设计的错误，后来都被证明是正确的。比如，精心挑选的Koblitz（科布利茨）曲线，避开了美国国家安全局在加密标准中暗藏的后门；比如，在椭圆曲线数字签名算法加密的基础上，再哈希两次，足以应付量子计算机的威胁。这粗心的与精密的居然是同一个人。

2008～2011年的网络讨论中，中本聪的一言一行也伴随着比特币概念的成型与实现，当然还有那篇著名的并未发表在任何学术期刊上的“神秘的论文”。论文的简介如下：

“本文提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。虽然数字签名部分解决了这个问题，但是如果仍然需要第三方的支持才能防止双重支付的话，那么这种系统也就失去了存在的价值。我们在此提出一种解决方案，使现金系统在点对点的环境下运行，并防止双重支付问题。该网络通过哈希散列对全部交易加上时间戳（timestamps），将它们并入一个不断延伸的基于随机散列的工作量证明的链条作为交易记录，除非重新完成全部的工作量证明，形成的交易记录将不可更改。最长的链条不仅将作为被观察到的事件序列（sequence）的证明，而且被看作是来自CPU计算能力最大的池（pool）。只要大多数的CPU计算能力都没有打算合作起来对全网进行攻击，那么诚实的节点将会生成最长的、超过攻击者的链条。这个系统本身需要的基础设施非常少。信息尽最大努力在全网传播即可，节点（nodes）可以随时离开和重新加入网

络，并将最长的工作量证明链条作为在该节点离线期间发生的交易的证明。”

2008年11月1日深夜2：10，当时的中本聪也许是怀着欣喜之情，发出了题为“Bitcoin P2P e-cash paper”（比特币P2P电子现金论文）的邮件。在邮件中他给出了含有上述见解的论文的连接，重述了比特币的五个主要特性：

- （1）可以用点对点的网络解决双重支付（双花）问题；
- （2）没有类似铸币厂一级的第三方的信任机构；
- （3）使用者可以完全匿名；
- （4）可以用哈希现金形式的“工作量证明”来制造新的货币；
- （5）用于制造新货币的“工作量证明”机制同样可以用来预防双重支付。

一个伟大的社会实验从此开始！然而直到今天，世界上仍然没有人能找到他。即使加州大学洛杉矶分校金融学教授Bhagwan Chowdhry（巴格·乔杜里）已提名他为2016年诺贝尔奖经济学奖的候选人，或是瑞士小镇上的瑞信银行打出招牌：“欢迎来到达沃斯，中本聪！”

他的一生就像一个谜团，出现、闪耀、隐逸于茫茫人流。也许正如康奈尔大学教授萨若所评论的那样：重要的是中本聪的实际遗产。我们的银行基础设施已经过时了，自千年虫爆发重写代码以来就再未更新过。金融体系的透明度和可审计性极低。银行零售业自1959年以来鲜有创新，直到几年前才有所改观。即使在今天，银行依然为我们的钱提供残旧、难用的接口。我不会宣称比特币那样的虚拟货币是最终的解决方案，或者甚至是目前可靠的解决方案之一。即使最近有规划进行改进，比特币也不能扩展到世界各地，而且它在安全上面临着很大的困难。但它确实带来了一些新的技术思路，可以丰富我们的国际社会；这些思路中的一部分是中本聪发现的，另一部分是中本聪的前人发现的。负责任的媒体需要放下毫无意义的寻人工作，把精力集中在比特币这种技术和它带来的启示上。这才是真正该做出的行动。

波动的价格，轰动的交易

从横空出世到渐入佳境，从默默无闻到妇孺皆知，比特币一路走来，价格的波动也一路备受争议。在看过了无数类似《十问比特币：3年翻25000倍》这样骇人听闻的新闻标题之后，人们的心脏承受能力也越来越强。25000倍，这是事实吗？

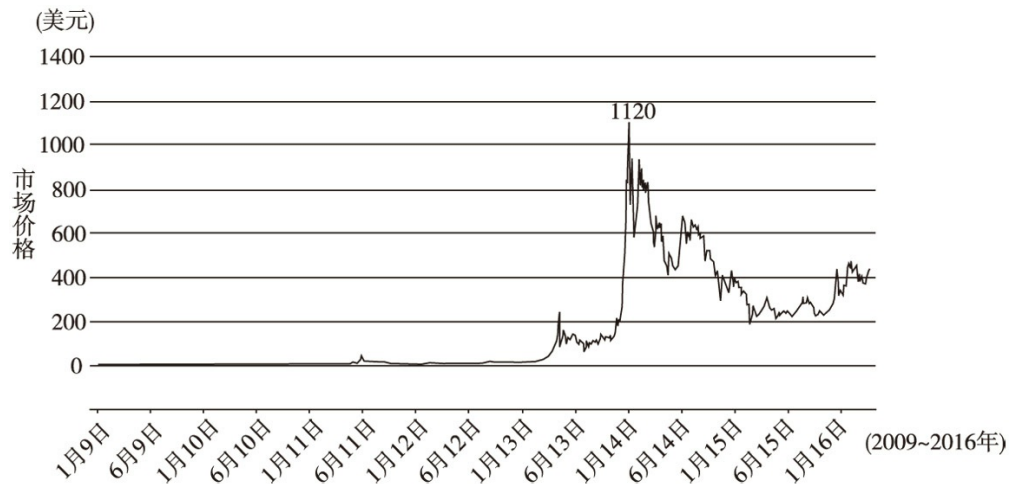


图1-2 比特币兑换美元价格

资料来源: [https://blockchain.info/zh-cn/charts/market-price?](https://blockchain.info/zh-cn/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=)

[timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=](https://blockchain.info/zh-cn/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=)

比特币兑换美元价格在2014年1月达到峰值1120美元左右。一般读者显然忽略了一个基本的数学常识: 如果一定要选用0作为除数, 进行对比, 则很容易得到一个近乎无穷大的结果。25000倍似乎也并不算离谱。我们不妨选用漫长的0值时期后非常早的一个点: 中本聪依然频繁出现的2010年的某一个点, 以0.0619美元作为基准, 做一下计算: 18093倍, 依然不小。

2016年2月25日比特币的价格是424美元, 虽然波动已经平缓, 但相对于两年前顶峰时期的1120美元, 也仅是那时的37.8%。其实从2011年第一次“比特币—比萨饼”的公开交易兑换至今, 比特币兑换美元价格经历了无数次的暴涨暴跌。

表1-1 2010~2015年比特币兑换美元价格

日期	1 个比特币 可以兑换 多少美元	备注
2010 年	最低 0.0025	在比特币论坛“bitcointalk”上，用户群自发进行交易，产生了第一个比特币公允汇率。该交易是一名用户发送 10000 比特币，购买了一块价值 25 美元的比萨饼。比特币公开交易开始时，其汇率主要参考 MTGOX 交易所内比特币与美元的成交汇率。
2011 年	最低 0.01	为了打破全球权威集团的金融封锁，维基解密刚宣布接受比特币捐助，全球最大的交易网站 Mt. Gox 就被黑客攻击，当时比特币价格迅速降到 0.01 美元/比特币。
2012 年	最高 33 美元	2012 年 11 月以前，比特币的最高汇率为 33 美元；在 2012 年 8 月，比特币的汇率为 10 美元左右；11 月底，比特币的汇率为 12.5 美元左右。
2013 年	最高 1200 美元	3 月 30 日，全部发行的比特币按市价换算为美元后，总值突破 10 亿美元。比特币的汇率由 2 月的 20 美元急升至 4 月的 180 美元，据此按照已经产出的比特币总数来计算，比特币的总市值约为 20 亿美元。5 月 30 日，Facebook（脸书）前高管 Chamath Palihapitiya（查玛斯·帕里哈皮迪亚）在彭博社发表文章预期，比特币将在 10 年内升值 3000 倍。11 月 28 日，比特币成交价首次突破 1000 美元。12 月 1 日，比特币上涨 521%，价格首次超越 1 盎司黄金价格。
2014 年	750~1000 美元	2014 年中旬，比特币汇率又一次因为比特币交易所 Mt. Gox 遭到黑客袭击急剧波动。原因是忽略了 2013 年 2 月 19 日发行的更安全可靠的比特币 0.8.0 系统，没有及时更新自己的 2011 年操作系统，为黑客带来可乘之机。
2015 年	250~500 美元	2015 年初，比特币价值在 250 美元左右徘徊，随后数月价格也没有大幅上涨。但 9 月比特币开始上涨。最急剧的变化发生在 11 月初，11 月 4 日比特币盘中一度上涨 20%，最高飙升至 500 美元。

数年间持续反复的涨跌后，大众终于接受了比特币这样的新常态，每日交易的次数也在震荡中逐步攀升，趋于 27.5 万笔 / 日（数据源于区块链网站）。

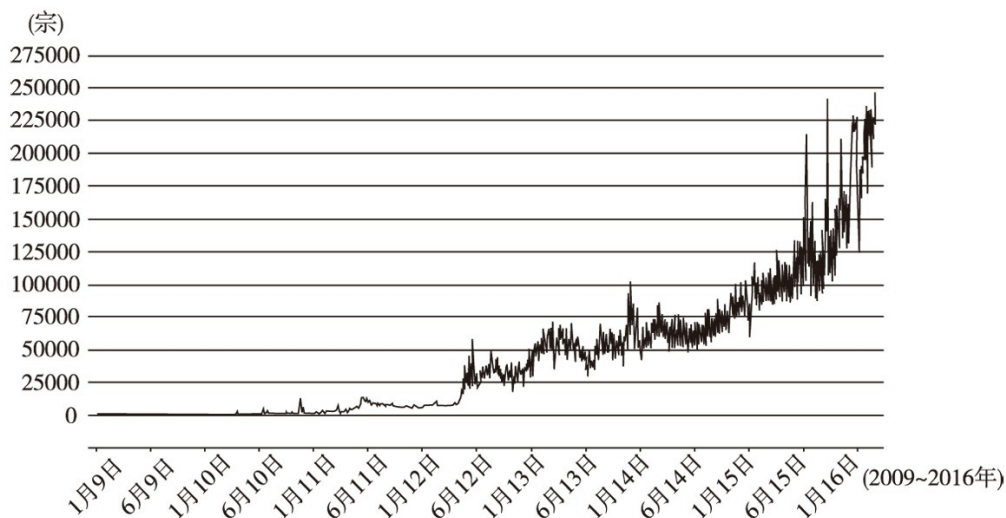


图1-3 比特币每日交易数

资料来源: [https://blockchain.info/zh-cn/charts/n-transactions?](https://blockchain.info/zh-cn/charts/n-transactions?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=)

[timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=](https://blockchain.info/zh-cn/charts/n-transactions?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&addr=)

核心开发成员埃米尔·塔吉 (Amir Taaki) 的评论中引用了业界周知的Hype Cycle (炒作周期) 来解释这一经济现象: “你可以说, 比特币遵循了市场研究机构Gartner (高德纳) 的‘炒作周期’规律, 即一种理论上的技术从被采用到成熟的曲线。这个周期始于技术萌芽期, 然后经历期望膨胀期、幻觉破灭谷底期、复苏期和生产力成熟期四个阶段。”根据这一理论, 比特币正在走出幻觉破灭谷底期, 人们开始珍视可靠的代码, 抛弃人为因素和围绕这种因素的动荡。

传输价值的代币

2016年中国人民银行行长接受财新传媒的采访中罕见地对区块链和数字货币进行了表态: “从历史发展的趋势来看, 货币从来都是伴随着技术进步、经济活动发展而演化的, 从早期的实物货币、商品货币到后来的信用货币, 都是适应人类商业社会发展的自然选择。作为上一代的货币, 纸币技术含量低, 从安全、成本等角度看, 被新技术、新产品取代是大势所趋。特别是随着互联网的发展, 全球范围内支付方式都发生了巨大的变化, 数字货币发行、流通体系的建立, 对于金融基础设施建设、推动经济提质增效升级, 都是十分必要的。”我们不难发现, 中国人民银行已经完全意识到了数字货币是新时代发展的必然, 而区块链则是一种可选项。

国际货币基金组织 (IMF) 与各国央行撰写的《数字货币》报告中提出了一种代表绝大多数央行的典型看法。国际清算银行下属组织CPMI (支付与市场研究委员会) 指出, 比特币隶属于数字货币的一种, 可以从以下三个维度来看待这种数字货币。

第一，它是一种资产，这一点如同其他很多货币一样，可以被用来作为支付的手段，但同时并不与一种主权货币必然相联系，没有任何实体、任何官方权威的背书（这一点与QQ币、网络虚拟币不同）。

第二，它并不具有内在固有的价值，因此它应有的价值取决于愿意接受它、使用它的人们，取决于这些人们对于它未来（可以兑换的商品、服务、货币）的信心。

第三，目前参与其中的第三方机构大都由“非银行组织”构成，这些组织在开发和维护数字货币和分布式账本技术上非常活跃。

在比特币开发和部署时需要考虑的因素中，这份报告同样提到网络效应（network effect），如同电话、手机第一次走入人们的世界，使用的人群越多，它的价值也随之越大。当越来越多的人采用比特币的时候，它的价值也会越大。而这源于它固有的优势：

（1）最初设计上考虑到了方便、全球可达、全球跨国界的使用；

（2）廉价。（各国央行也承认至少在某些交易的场合，对于用户来说，它提供了一种更加方便和廉价的方法）

在各国央行看来也有悲观的一面，它也有着安全和信任主体缺失的缺点。但这些都不妨碍比特币作为一种传输价值的代币或传输价值的语言继续发挥作用。

然而在自由主义者眼中，比特币显然走得更远，它不仅可以被作为一种安全可靠的存储和转移法币价值的机制，更是一种互联网协议上的价值操作方法（Value over IP）。比特币以一种全新的方式取代物权法中的传统产权链，以一种可识别的安全方式保护使用者的资产利益，并提供一套透明的规则和执行机制以便所有参与者在记账上受到平等对待。所有这些比特币完成的功能都不需要依赖金融、监管或司法部门，比特币本身就是法律的代码。这一点尤其在缺乏完善的金融系统、法制失灵、无法保证公民财产权稳定的地方，体现得淋漓尽致。

使用Kipochi钱包的肯尼亚人不仅可以如愿地使用比特币的全球性金融体系，而且还可以把比特币兑换成M-Pesa以便完成当地的交易和购物。新时代里远下南洋掘金的菲律宾、马来西亚华裔可以通过OKlink将东南亚货币以低廉的手续费用转回中国大陆的家中。

在政府和私营部门已经失败的地方，开源开发已经在比特币身上找到了解决办法。我们回首它诞生的历史也会发现，比特币在2008年开始的国际金融危机中，在普遍的泡沫和对权威信任的丧失中诞生，可以说不仅是比特币开发者造就了比特币，而是这个时代造就了比特币。

区块链到底是什么

比特币的传奇尚未落幕，另一个传奇就已经开启：2015年7月，高德纳发布了新一年的技术成熟度曲线。从图中可以清晰地看到：比特币所代表的加密货币（cryptocurrencies）和虚拟货币交易（Cryptocurrency Exchange）逐渐从2014年炒作的顶峰期跌落到大众普遍失望的谷底。

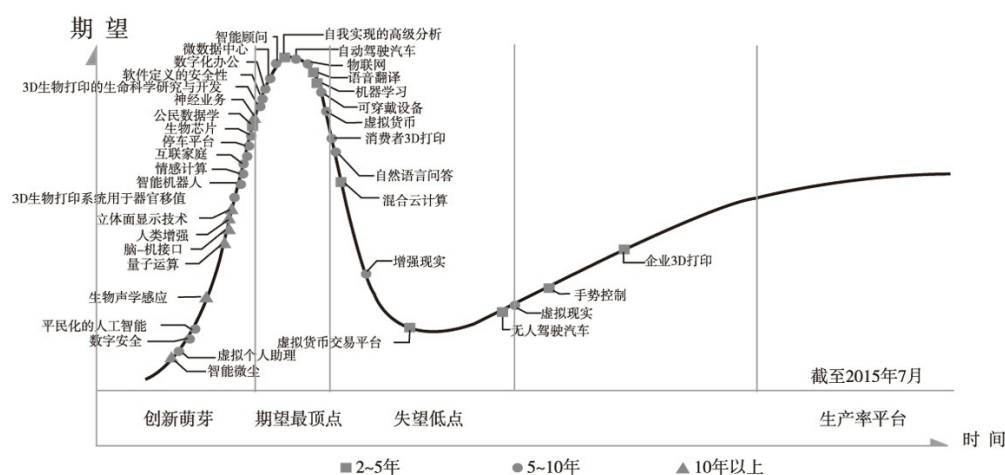


图1-4 高德纳2015年新兴技术成熟度曲线

资料来源：<http://www.gartner.com/newsroom/id/3114217>

中文版链接：<https://www.zhihu.com/question/21314303>

然而，出乎意料的是，整个产业并未衰落。截至2016年2月19日，全球比特币相关产业投资额度仍然逐渐升温，突破10亿美元。这其中以完成两轮融资的OKcoin为首的7家中国公司也格外引人注目，带领着中国区块链产业的发展。这也显示了资本与市场的整体乐观。正如中国人所说的，“阴极阳生”。一种新的技术让投资者和业界再次看到了曙光，那就是Blockchain（区块链）。这是一个并不常见的现象。一般而言，当一项技术衰退的时候，除非它的生命周期非常长，能极大地激励人类的期待和梦想，比如人工智能，它能极大地勾起科研界、技术界的梦想。从20世纪60年代，从海曼·明斯基（Hyman Minsky）时代一直发展到今天的阿尔法狗时代。但大部分创新技术一跌下去就被淘汰了。比特币、加密货币这种技术之所以能硬挺到今天，非常重要的因素就是背后的区块链技术又再次把它拉动了起来。

表1-2 中国区块链产业投资列表（2016年2月19日更新）

日期	公司	类别	融资规模 (百万美元)	累计资金 (百万美元)	融资轮	投资人	总部	国家
2014 年 10 月 10 日	Melotic	交易所	1.18	1.18	种子轮	Ceyuan Ventures, Lightspeed China, Bitcoin Opportunity Corp, 500 Startups, Marc Van Der Chijs	香港	中国
2014 年 5 月 27 日	Huobi	交易所	10.00	10.00	第一轮	Sequoia Capital China	北京	中国
2014 年 3 月 26 日	Hive	钱包	0.19	0.19	种子轮	Roger Ver, Seedcoin	香港	中国
2014 年 3 月 16 日	OKCoin	交易所	10.00	10.60	第一轮	Ceyuan, Mandra Capital, Ventureslab, PreAngel, Individual Investors	北京	中国
2014 年 3 月 7 日	CoinSimple	通用 支付	0.18	0.18	种子轮	Seedcoin, Individual Investors	香港	中国
2014 年 2 月 4 日	BltSim	处理器	0.50	0.50	种子轮	Seedcoin, Individual Investors	香港	中国
2013 年 11 月 18 日	BTC China (Shanghai Satuxi Network)	交易所	5.00	5.00	第一轮	Lightspeed China Partners, Lightspeed Venture Partners	上海	中国
2013 年 9 月 4 日	OKCoin	交易所	1.00	1.00	种子轮	Ventures Lab	北京	中国

比特币与区块链是父与子关系吗

对于比特币与区块链，有两种常见的错误概念，在业界广为传播：

错误观念1：比特币与区块链是父与子的关系；

错误观念2：区块链是比特币的一个意外发现和生成物，带来出乎大家所料的惊喜，之前没有人料到这一切。

事实上，作为比特币实现的底层技术，区块链的产生是伴随着比特币一道出现的，称之为父与子的关系极其不准确。其次，与其说意外，倒不如说是“蓄谋已久”。早在2010年，在后来

的比特币核心开发者Gavin Anderson（盖文·安德森）的讨论帖中，中本聪就指出自己为什么在比特币初始代码版本wallet.dat中嵌入一种非常简单的脚本（Gavin发现后曾一度陷入紧张不安中）。

中本聪说：“我很多年前就已经在思考，是否可以让（比特币）支持多种交易类型，包括：托管交易、债券合同、第三方仲裁、多重签名等。如果比特币未来能够大规模发展，那么这些交易种类都将是未来想探索的，但是在一开始设计时就应该考虑到这些交易，这样奖励才能够实现。”

事实上，正如后来的研究者分析发现，这些结构的应用早已超出了数字货币，甚至可以扩展到任何类型的交易方式，例如各种基于智能合约的应用。其实可以套用设计中的专门术语说，“区块链”是比特币的“可供性”，这种载体提供了一种更为广阔的交互的可能性。

中本聪版本的第一版“比特币区块链”的基础协议非常简单：通过盖时间戳，各方一同记账、一同公证，每10分钟确认一次，形成记录全网这10分钟所有正确的一个账本数据库“区块”，然后每个合法的区块连成一个个链条，形成分布式的、大家一致同意的账本数据库，这就是“区块链”。

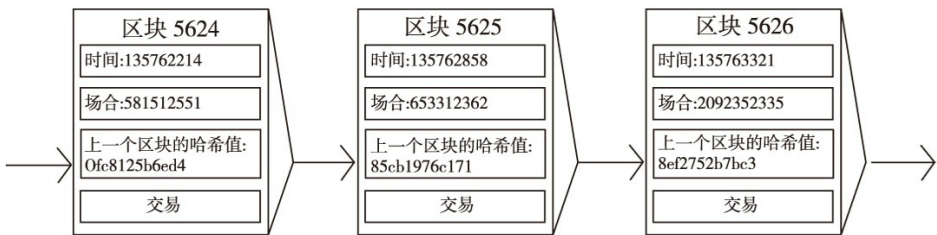


图1-5 区块链示意图

资料来源
<https://camo.githubusercontent.com/e8e2a0c15c17b066e7f17056f7697819b9a1aa33/6874747f>

区块链本质上是一个去中心化的分布式账本数据库，是比特币的底层技术，和比特币是相伴相生的关系。区块链本身其实是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。

每当有加密交易产生时，网络中有强大运算能力的矿工（Miner）就开始利用算法解密验证交易，创造出新的区块来记录最新的交易。新的区块按照时间顺序线性地被补充到原有的区块链末端，这个账本就会不停地增长和延长。

通过复杂的公共钥匙和私人钥匙的设置，区块链网络将整个金融网络的所有交易的账本实时广播，实时将交易记录分发到每一个客户端，同时还能保证每个人只能对自己的财产进行修改。当然，账本里也有别人的交易记录，虽然可以看到数值和对应的交易地址（基本上这是由

一段冗长的乱序字母和数字组成），但是如果不借用其他技术手段也根本无法知道交易者的真实身份。

如果从不同的技术角度来剖析，我们可以这样看待区块链：它是一种数据库、一种分布式系统，也是一种网络底层协议。

（1）数据库。区块链是一种公共数据库，它记录了网际间所有的交易信息，随时更新，让每个用户可以通过合法的手段从中读取信息，写入信息。但又有一套特殊的机制，防止以往的数据被篡改。

（2）分布式系统。区块链是一种分布式系统，它不存储放置在某一两个特定的服务器或安全节点上，而是分布式地存在于网络上所有的完整节点上，在每一个节点保留信息备份。

（3）网络底层协议。区块链是一种共识协议，基于这种协议，可以在其上开发出数目繁多的应用。这些应用在每一时刻都保存一条最长的、最具权威的、共同认可的数据记录，并遵循共同认可的机制进行无须中间权威仲裁的、直接的、点对点的交互信息。

层出不穷的其他数字货币

由于区块链最先被应用于数字货币——比特币，所以各方的开发设计者很容易想到，运用或改造这种区块链技术（加密算法、处理时间、区块大小等）可以造出新的数字货币，我们不妨称之为1.0时代。1.0时代中各种数字货币层出不穷，截至2016年2月28日，统计显示已知的有688种，从分文不值到估值上亿美元。我们简要介绍除比特币以外排名靠前的三种。

表1-3 全球排名前十位的数字货币

▲#	名称	符号	市值	单价	可用供应	交易量(24小时内)
1	Bitcoin (比特币)	BTC	\$ 6,514,507,943	\$ 426.92	15,259,425	\$ 43,392,600
2	Ethereum (以太坊)	ETH	\$ 498,257,063	\$ 6.44	77,370,190	\$ 9,355,050
3	Ripple (瑞波币)	XRP	\$ 268,466,739	\$ 0.007875	34,090,841,338	\$ 559,169
4	Litecoin (莱特币)	LTC	\$ 151,026,370	\$ 3.38	44,689,101	\$ 750,248
5	MaidSafeCoin(玫德币)	MAID	\$ 44,112,139	\$ 0.097474	452,552,412	\$ 2,331,570
6	Dogecoin (狗狗币)	DOGE	\$ 25,452,545	\$ 0.000246	103,268,327,584	\$ 191,987
7	Dash(达世币)	DASH	\$ 24,954,884	\$ 3.99	6,252,273	\$ 137,445
8	Peercoin(点点币)	PPC	\$ 10,721,694	\$ 0.465793	23,018,153	\$ 49,654
9	BitShares(比特股)	BTS	\$ 10,075,647	\$ 0.003960	2,544,233,346	\$ 92,221
10	Monero(门罗币)	XMR	\$ 9,664,070	\$ 0.866732	11,150,010	\$ 145,885

资料来源：<http://coinmarketcap.com/>

1. 以太坊 (Ethereum)

以太坊是下一代密码学账本，支持众多的高级功能，包括用户发行货币、智能协议、去中心化的交易、普遍认为的第一个完全的去中心化自治组织 (DAOs) 或去中心化自治公司 (DACs) 应用。使以太坊与众不同的是实现这些功能的方式。以太坊并不是把每一个类型的功能作为特性来特别支持，相反，以太坊包括一个内置的图灵完备的脚本语言，允许通过被称为“合同”的机制来为自己想实现的特性写代码。一个合同就像一个自动的代理，每当接收到一笔交易，合同就会运行特定的一段代码，这段代码能修改合同内部的数据存储或者发送交易。高级的合同甚至能修改自身的代码。

2. 瑞波币 (Ripple)

瑞波币是Ripple网络运行的基础货币，就像比特币一样可以在整个网络中流通，而不必局限于熟人圈子。瑞波币引入网关系统，它类似于货币兑换机构，允许人们把法定货币注入、抽离Ripple网络，并可充当借贷双方的桥梁。

3. 莱特币 (Litecoin)

莱特币与比特币相比具有三种显著差异：第一，莱特币网络大约每2.5分钟（而不是10分钟）就可以处理一个块，因此可以提供更快的交易确认；第二，莱特币网络预期产出8400万个莱特币，是比特币网络发行货币量的四倍之多；第三，莱特币在其工作量证明算法中使用了由Colin Percival（科林·珀西瓦尔）首次提出的Scrypt加密算法，这使得相比于比特币，在普通计算机上进行莱特币挖掘更为容易（在ASIC矿机诞生之前）。每一个莱特币被分成100000000个更小的单位，通过8位小数来界定。不同于比特币，Scrypt所具有的内存密集特性让莱特币更适合用图形处理器（GPU）进行“挖矿”。为Scrypt实施的FPGA（现场可编辑逻辑门阵列）和ASIC（专用集成电路），相比于比特币使用的sha256，更为昂贵。

区块链的实际应用

比特币也许是区块链上最著名的应用，除了比特币以及以它为代表的数字货币之外，近年来也涌现出了许多其他应用。我们也将会在后面的章节展开财产、物流、存储、选举等各方面应用案例的详细说明。这里仅仅给出部分例子，略微彰显它广阔的前景：美国在线零售商Overstock就基于区块链开发了一个名为“tØ”的股权交易平台。在同一领域，纳斯达克宣布与Chain达成合作协议：它们正试图用区块链来颠覆股票交易市场。与此同时，高盛和巴克莱等金

融机构目前也在联手创业公司，为市场开发一种基于区块链的新框架。

许多创业公司又在此基础上更进了一步，计划利用区块链来交易实体资产。比如，Bitproof和Blocknotary试图通过在区块链上记录合同交易来颠覆这些行业，他们不是在公证人面前完成房屋买卖，而是将合同保存在公共账单上。

另外，Colu正在利用区块链，通过数字令牌（digital token）来管理资产——数字令牌可以开启在线服务或实体资产。

这项技术还可以被应用于知识产权领域。例如，Verisart正在利用这种分散式技术来验证艺术作品的真伪。它给艺术作品相应的版权编码，然后将它们记录在区块链中。另外，Proof of Existence还利用公开账单追踪用户创建的档案。

区块链还可以用来验证人的身份。ShoCard会给个人身份信息编码并进行保存，还能实现合同的智能化管理：这得益于这种分散式基础设施，一旦满足了某些条款，合同会得到自动处理。IBM目前正在开发这种应用，该公司还公布了与三星ADEPT的合作计划——ADEPT是一个在物联网领域使用区块链技术的概念验证。

区块链的颠覆特点

“如果我知道我将在何处死去，我将不去那个地方，这样我就可以得到永生。”这是著名投资人查理·芒格（charlie Munger）经常引用的一句俏皮话，其中充满了深深的、反向思考的智慧。如果我们今天希望了解区块链的种种特性所带来的去中心化、分布式等对于传统的颠覆，我们不妨思考以下两个问题：传统的方式意味着什么，或者说中心化意味着什么？集中式又意味着什么？我们设想一个例子，假定在10000年前，我手里有一个贝壳，对方有一袋盐，我俩简单直接地换走，而我们不需要知道过多对方的信息，也不需要知道对方的家庭住址、身份证、信用等冗余信息。我的东西对他有价值，他的东西也对我有价值，我就可以直接跟他请求交换。但后来随着社会的不断发展，复杂以及不必要之物充斥到我们的价值传输网络中。现在，我们做一个非常简单的交换过程，必须依赖银行或下面例子中的钱庄。首先把我们的价值转化为银行记账单位，然后通过一个中心化的节点银行，进行这种价值的传输。

我们看一下极端中心化集中式的处理方式。

第一步，登记你（持贝壳少年）的姓名、年龄、身份证、住址、工资，提供给中心化钱庄。

第二步，登记他（持盐少年）的姓名、年龄、身份证、住址、工资，提供给中心化钱庄。

第三步，你把贝壳寄往钱庄。

第四步，卖盐的少年把盐寄往钱庄。

第五步，钱庄把盐寄给你。

第六步，钱庄把贝壳寄给对方。

第七步，钱庄把你们两人的信用值各自+1，并在钱庄内保管你们的信用记录。

而去中心化、分布式处理方式：你和少年交换盐和贝壳，并不需要太多其他信息，交易地址、金额记录登记更新到区块链上。

我们不难看出，在某些特定的场合，去中心化分布式处理，不仅更加便捷，而且也更加自主。你并不一定需要一个掌握你所有信息，甚至与交易无关的毫不必要的信息的中心化代理（钱庄）来协调处理你的一切交易。这不仅是不安全、不便捷的，还可能造成信息不对称，甚至被“中心”反向控制，因此也是不必要的。

贝尔的电话技术、20世纪90年代的互联网的颠覆性来源于它们所带来的便利，对人类生活和行为的巨大改变。有了电话和手机，我们就可以端对端及时发送信息进行通信；有了互联网、微信和QQ，语音、文字、视频等“信息”和“数据”才可以方便传播，使人们之间的联系和网络更加直接、便捷。总体而言，传递“消息”的网络已经非常发达、直接、便捷、流畅。但是现在我们在传递钱、资产这样的“价值资产”时，我们的网络还处于一个十分臃肿、低效的状态，某些方面甚至不如原始社会时贝壳与盐等物物交换的网络。

可以发现，区块链就是一个“去中介化”的“价值传输网络”。如果说“拜占庭将军问题”揭示出了我们分布散落的个体节点之间信息传达与协同的困难，那么区块链就是一种解答，迄今为止最有力、最清晰、最具有现实性的一种解答。它解构了信任代理（中介）存在的必要，提供了另一种点对点直接交互的可能。就像我们在原始社会中一样，真诚地面对面地交互，不需要任何中介，甚至不需要双方的信任，只需要有限的了解，便可以来去匆匆，相忘于江湖，其中的交互皆留给底层。这使交易乃至一切交互更方便、更有效率。在一个一个点看，这只是个体之事，但从更高的维度看，它也使大规模的、无中介的协同交互成为可能。不再需要强权、巨大中介的集中智能处理，而智能则隐于底层、隐于链条、隐于各处。它不是庞然大物似的存在，但又细微地无所不在，这种智能终将重新塑造出我们商业、文化乃至整个社会的未来。

注释：

[\[1\]](#) 来自维基百科。

[2]在数学和计算机科学之中，算法为一个计算的具体步骤，常用于计算、数据处理和自动推理。

第二章 区块链

——颠覆世界的力量

区块链生成后，一路令人惊奇，不仅仅在于它对于当下世界的改变，更在于它塑造未来的可能。它像一个具备智能的集群，不断演进出颠覆性的力量。虽然它散落，但并不散乱与无序，而更像一个协调有序发展的，最终具备智慧的有机群体。这种现象在自然界中也有存在。

颠覆的核心——去中心化

自古以来鸟类都是一个非常有智慧的群体，每当到了迁徙的时间，候鸟们都会成群结队地从寒冷的北方飞到温暖的南方过冬，鸟群通常要飞几十天才能到达过冬的目的地。如果需要长时间迁徙的不是鸟群而是人群呢？那么就需要高科技设备帮助指路，并且还需要选出一个领导人来带队。

飞行途中的一只鸟对自己的鸟群形态并没有全局概念，结队飞行的鸟儿对鸟群的飞行姿态和聚合也是视而不见的。“群态”正是从这样一群完全罔顾其群体形状、大小或队列的生物中涌现出来的。科学报道记者詹姆斯·格雷克（James Greek）曾经写道：“单只鸟或一条鱼的运动，无论怎样流畅，都不能带给我们像玉米地上空满天打旋的燕八哥或百万条鳊鱼鱼贯而行的密集队列所带来的震撼。（鸟群疾转逃离掠食者的）高速电影显示出，转向的动作以波状传感的方式，以大约1/70秒的速度从一只鸟传到另一只鸟，比单只鸟的反应要快得多。鸟群远非鸟的简单聚合。

群鸟们履行着一条非常简单的原则：彼此只看周围大约6只同伴的行为，只要和它们保持一致就行。于是，我们看到，罗马上空的欧洲椋鸟像巨大的礼花爆炸，在空中绽放，却彼此牢固地粘在一起；随即又像一朵游动的云，飘到其他地方，继续绽放……

沙丁鱼也和欧洲椋鸟相似。海洋里面有许多厉害的大家伙，像鲨鱼生活在食物链的最上层，弱势的沙丁鱼是如何抵御天敌的呢？它们没有任何的捕猎能力，也没有躲避能力，这些沙丁鱼在大自然的进化中形成了“群体效应”。当天敌鲨鱼、海豚冲过来时，它们会聚拢在一起形成一个群体，而且这个规则非常简单，每一只沙丁鱼只要盯紧它周围前后左右的鱼，与其保持相同的距离和方向。当天敌扑向沙丁鱼群时，鱼群的变化会让天敌变得不知道该捕捉哪一只。每一条沙丁鱼都在重复着自己的本能，而当全体沙丁鱼都正确地做出动作时，它们就变成了一个整体。沙丁鱼群完全是一个去中心化的体系，这个体系可以让它们在残酷的自然界中生存下来，不断进化。

蜂巢是由一只蜂王和许多工蜂组成的，看似是一个蜂王领导工蜂的组织，但是，蜂王的任务只是繁衍后代，而不参与其他一切生产活动，也不领导工蜂。那么工蜂们是怎样在没有领导的情况下统一工作，并且建立蜂巢的呢？原因在于基因。每一只工蜂在出生的时候都知道该如何建立蜂巢，如何寻找花蜜，并不需要任何的引导。

鸟群、鱼群、蜂群可以说是自然界的超级团队，它们没有管理者，也不需要领导人，只要遵循简单的法则，就能完成许多不可思议的复杂任务。数亿年的进化淬炼，让它们发展出各种

绝妙的策略，使它们成为拥有智慧的群体。它们的神奇在于，有一只看不见的手，一只从大量愚钝的成员中涌现出来的手，控制着整个群体。它的神奇还在于，量变引起质变。

要想从单个虫子的机体过渡到集群机体，只需要增加虫子的数量，使大量的虫子聚集在一起，使它们能够相互交流。等到某一阶段，当复杂度达到某一程度时，“集群”就会从虫子中涌现出来。虫子的固有属性就蕴含了集群，蕴含了这种神奇。我们在蜂箱中发现的一切，都潜藏在蜜蜂的个体之中。尽管你可以用回旋加速器和X光机来探查一只蜜蜂，但是永远也不能从中找出蜂巢的特性。

而区块链的种种特性——去中心化、共识、分布式所形成的规则，使原本散落在全球的交易数据，第一次在网际间流动聚合，涌现出一个价值数据的巨大“鸟群”，也演化出其自身的种种智能。

去中心化——“鸟群智慧”的一角

我们人类没有这样的基因，我们目前还是生活在中心化的世界里。但是我们有幸接触到了去中心化也就是“鸟群智慧”的一角——区块链。

在中心化的世界里，大家都知道地球围绕着太阳转、国家有元首、学校有校长、连酒店也有总经理，但在我们生活中存在着无数的去中心化的系统，分布在我们生活中的各个方面。去中心化的系统还有一个专业的词汇叫分布式自治系统。

1. 区块链技术的一个突出特点是去中心化

在一个分布有众多节点的系统中，每个节点都具有高度自治的特征。节点之间彼此可以自由连接，形成新的连接单元。任何一个节点都可能成为阶段性的中心，但不具备强制性的中心控制功能。节点与节点之间的影响，会通过网络形成非线性因果关系。这种开放式、扁平化、平等性的系统现象或结构，我们称之为去中心化。

自穴居的原始人在墙壁上涂鸦时起，人类就一直有记录信息的需求。后来出现了用图书来记录知识，用账本来记录财务债务。到了近代，会用录音机记录声音，用胶卷记录图像。随着互联网数字化的到来，记录方式发生了巨大改变，变得数字化、虚拟化。电子书、电子地图、电子相册、影视综艺节目也实现了数字化网络传播。

然而，这些记录形式的背后有个共同的深层问题——中心化。中心的重要性在我们心中不言而喻，中心是一个集中所有资源和数据的地方，是所有路径的交错点。中心的意义在于控制。尤其是在工业时代，人们将生产和工作都集中在一起，从而达到完全控制的目的。中心能

够控制所有的过程，保证准确和无误。

但是中心化也同时存在着致命的缺点。比如在一个中心化的国家，国王是整个国家最中心的人物，整个国家运转的过程都要经过国王的处理，这中间就出现了问题：如果国王是一个非常无能的人，下达的指令是愚蠢错误的，但国王是整个国家的中心，即使国家所有的人都觉得国王的指令有问题，也必须去执行；就算国王下达了一个非常英明的指令，所有的人都觉得非常不错，但是指令从中心传达到底层要经历很多结构和环节，可能指令在经过一层一层的传递到达最后的执行环节时已与最初的指令产生偏差，造成最后的执行结果与最初的指令预期完全不同。并且信息在传递的过程中需要时间，有可能信息从中心点发出后在到达执行点的时候已经错过了最好的执行时机，导致结果大打折扣。

现在的一些传统企业也存在着中心化的问题。通常一家公司不是私有制就是股份制形式，登记注册于中心化的政府机构。中心化的董事会成员聚集在总部运营管理这家公司的所有事物。这家公司的组织架构是自上而下、等级明确的，首席执行官（CEO）几乎控制着公司的所有决策。这就存在上述中心化所导致的问题，权力的集中容易导致底层执行积极性下降，管理层容易滋生腐败，信息传递容易出现滞后及不准确性。越来越多的公司开始思考如何解决中心化所带来的问题，去中心化或许就是答案。

在互联网的建设过程中，互联网的创造者们曾想过设立一个中心来交换数据，但这个方案很快就被否定了。因为互联网有巨大的数据需要处理，设立一个中心虽然达到了绝对控制的目的，但将引出更多的问题。一个中心来处理整个互联网的数据，将使得这个中心非常容易发生错误和故障，而一旦这个中心出现问题，便会导致整个互联网崩溃，造成极大的问题。于是互联网被设计为无中心的形式，从而使其效率大大提高。

虽然采用无中心的形式，整个系统看似处于“失控”的混乱状态，会频繁出现许多小错误，但这样的形式却可以避免互联网出现大的错误，这便是去中心的意义。在加密货币的某些领域，“去中心化的自治公司”（DACs）或“分布式自治组织”（DAOs）正流行。比特币同样被视为去中心化货币。DACs让全世界的各个角落、各行各业去中心化成为可能，比如在商业、贸易、金融和经济方面。这种类型的公司由顾客和员工共同拥有并经营，没有高高在上的老板，没有中心集权的机构充当董事会的角色。对于一些忙碌生活的人来说，这是通往自由自主道路的巨大进步。

人类进步的历史几乎可以说是信息传递不断变革和升级的历史，从早期没有文字到发明文字，从发明文字到鸿雁传书，从印刷术的发明到电报电话的崛起，从有线通信到无线通信的升级，其本质上都没有改变传递的点对点的单向模式。而互联网的兴起则实现了信息传播的多点、全方位、全天候、不间断的全球网络化，其革命性的意义在于打破了传播的单一中心模式。

2. 没有中心的本质就是人人都是中心

在互联网的冲击下，人类的文化模式正全面走向碎片化。以前任何一个社会都是单中心社会，比如原来我们了解信息要看高大上的媒体，因为它们传统社会的信息中心，是权威。现在一切都变了：年轻人不再仅仅看电视，而是在互联网、手机上随时随地接收信息、随时随地发送信息、随时随地制造信息、随时随地娱乐信息。所以每一台电脑、每一个手机、每一个人都变成一个信息中心，整个人类社会变成了多中心社会，人类进入了“多中心时代”。

为什么去中心化一定会成功

在这个世界上，中心化形态已经存在太久了，从上古社会以血缘关系建立起来的部族部落，到古代封建社会的王权社会，再到近代社会的资本主义、社会主义制度。这些其实都是不同形态的“中心化组织”。

以上所描述的人类社会形态的更替，其实就是一步步淡化中心化的历史进程。

人类的历史进程中，每个人能够独立运作的事情变得越来越多，个人能够行使的权利实际上在逐渐增大。毫无疑问，当个人的能力能够足以完成社会运作时，中心化的大机构、大组织存在的必要性也会变得越来越弱。

去中心化从信息传播的角度已经取得了某种程度的成功，尤其是网络媒体，已经成功淡化了传统信息传播金字塔中的“信息中心”，而让原来传播中的“受众”成为新的信息源，人人都是中心。举例来说，新华社、新华网、人民网、纽约时报、新浪网、雅虎等都是传统意义上的“信息中心”。如今博客、微博、社交网络的崛起，让网友们自发维护的这些信息平台成为新的信息中心。无论从哪个角度看，网络上人人都是中心的格局已经基本形成。以前人们围绕在收音机旁听广播，坐在电视前看新闻联播的时代一去不复返。

去中心化能够降低维护成本，调动每个成员的参与积极性。我们大胆预言，未来的很多东西，都将走上去中心化之路。比特币作为去中心化的第一种数字货币，不过刚刚走出万里长征的第一步，未来要走的路还很长。

区块链的去中心化技术意味着什么

区块链就是一个网络记账本，不过由于伪造成本极高，理论上不会存在被伪造的信息。因

此区块链技术受到了很多投行的青睐，全球顶级的九大投行都在投入巨资做研发。区块链的数据区块取代了传统的服务器，使得每个参与区块链系统的节点都是主机，所有的数据变更和所有的交易信息都被记录在云系统上。从理论上来说，它是一个证明与自证的系统。

例如我们每个人都网购过，买家买东西的时候，需要把钱打给淘宝等电商，淘宝等电商平台充当一个中介机构，托管了买家的资金，卖家看到买家已经打款给淘宝，于是去发货，等买家收到货后，会有一个确认收货的机制，中介电商再将买家之前托管给他们的资金转给卖家。这个方式非常复杂，而且很烦琐，卖家回款的速度也比较慢，而作为中介的电商却赚得盆满钵满。

而区块链的出现，其实就是消灭这种中心化的系统。区块链是以点对点的模式进行交易，可以省略掉中心化的模式，直接让买家与卖家进行交易，通过计算机的程序实现物物相连的构想。

对去中心化进程的一个回应是分享。分享是去中心化进程的动词表达，这也是我们有很多分享社区的原因。我们可以分享数据、进程、影响力、信息，去中心化的结果即分享行为的增加。

未来，当大多数生产都能由机器人来完成时，再使用中心化的系统，就会导致大规模的失业。而使用去中心化系统，每个人都可以依靠自己的机器人养活自己，形成个人自给自足的经济模式，未来的可持续性发展空间是无限的。未来世界将会变成一个完全去中心化的世界，没有任何一个人或者组织作为权威或控制中心，或者说每一个人或组织都是中心，信息的流通效率将变得非常高，这对于世界来说无疑是一个巨大的进步。

区块链将构建完美的契约世界

在2030年一个明媚的上午，你漫步走入一个当地的杂货店去买牛奶。随着你的手一挥，你的智能手表检测到牛奶盒中内置的透明加密芯片，并且获得了它的哈希代码。这一瞬间，这盒牛奶就毫无争议地成了你的牛奶。未来，的确很有可能出现这样的情况：我们将不再使用现金买东西，也完全重新定义事物所有权的概念。

即使互联网已经通过各种方式在各个方面改变了我们的生活，但是从来没有一种方法能够真正地在没有中心化权威机构的授权下让你“拥有”某些数字产品。你在网上拥有的一切，从你的钱到你的身份，都需要一个公正的第三方机构才能证明，这是我们能真正证明拥有某物的唯一途径。从技术上讲，所有你的在线资产实际上都是你借用的。不过从现在开始，不再如此！

如果你真正拥有在线资产、能够降低抵押贷款利率、更加容易地更新遗嘱、贷款没有处理费用、买卖交易免手续费.....那会怎样？这些应用和其他更多的应用是智能合约向我们许诺的未来。由于密码学货币的出现，智能合约这一技术正越来越走近我们的现实生活。

智能合约是能够自动执行合约条款的计算机程序。未来的某一天，这些程序可能取代处理某些特定金融交易的律师和银行。智能合约的潜能不只是简单地转移资金。一辆汽车或者一所房屋的门锁，都能够被连接到物联网上的智能合约打开。但是与所有的金融前沿技术类似，智能合约的主要问题是：它怎样与我们目前的法律系统相协调呢？还有，会有人真正使用智能合约吗？

智能合约赋予物联网“思考的力量”

物联网是一个设备、车辆、建筑物和其他实体（嵌入了软件、传感器和网络连接）相互连接的世界。小到恒温器，大到自动驾驶汽车（如配有召唤模式的特斯拉Model S型轿车），这些都可以成为物联网的一部分。

电子商务网络平台“物联中国”预计未来10年，物联网的设备数量将达到1000亿量级。对于如此庞大的网络，如果以中心化的组网模式，数据中心的基础设施投入、维护成本将无法估量。在云计算尚未打消人们对数据安全的疑虑时，物联网的设备更加深入人们的生活隐私。比如：你家的电饭锅每天几点做饭、做几人份的、家里的热水器是几点开始工作的，这些数据如果都传输到管理中心节点，那么你的物联网方案又该如何应对呢？

现在的物联网还存在一些安全问题，如汽车系统可能会受到恶意攻击、房屋进入系统安全性需要加强、互联网的安全挑战等。区块链中的智能合约技术具有解决这些问题的潜力。首先，区块链的最大特点就是去中心化，运用区块链技术后，我们对智能设备发出的指令无须上传到网络的中心，因为我们每个人都是一个中心，指令只需要在我们中间进行循环，大大减少了信息流通的时间成本。其次，在信息安全上，智能合约也是无法被超越的，区块链技术的安全性能够保证我们在使用智能设备的时候信息不被其他人窃取，我们再也不用担心在网上借了一笔钱之后手机被垃圾贷款信息填满了。

从智能合约到智能资产

虽然智能合约仍然处于初始阶段，但是其潜力显而易见。想象一下，分配你的遗产就像滑动可调滑块就能决定谁得到多少遗产一样简单。如果开发出足够简单的用户交互界面，它能够解决许多法律难题，例如更新遗嘱。一旦智能合约确认触发条件，合约就会开始执行。在未来，智能合约将会改变我们的生活，我们现在所有的合约体系都可能会被打破。智能合约在未来可以解决所有的信任问题。

智能合约也可以用在股票交易所，设定触发机制，达到某个价格就自动执行买卖；也可以用在京东众筹这样的平台，合约可以跟踪募资过程，设定达到众筹目标自动从投资者账户划款到创业者账户，创业者以后的预算、开销可以被跟踪和审计，从而增加透明度，更好地保障投资者权益。

如果贷款还款由智能合约处理，那么贷款处理费用将被取消，最终的结果就会使得获得房屋所有权的成本更低。尽管你能通过一家银行获得抵押贷款，但是一般而言，银行不会持有长达30年的贷款，抵押贷款将被卖给投资者。银行只是成为你每月还款的处理者，向投资者支付大头，小部分交税，更小部分用于房主的保险。这只是一个非常简单的操作任务，但是银行经常需要一个季度到半年的时间来处理抵押贷款还款问题。银行只是从贷款者手里接受还款，将还款转交给投资者，并凭此服务向人们收费。但是，理论上智能合约能够非常容易地处理这种业务。

智能合约还可应用于个人健康管理。你可能会拥有一个可穿戴的健身追踪器，把卡路里数量和步数发送到区块链。数据是经过加密的，身份是匿名的。家用医疗设备也是如此，区块链会和健康专家例如教练、医生或者医疗机构建立联系，智能合约会触发需要的服务——不管是健身计划还是针对某些慢性疾病的治疗。

未来律师的职责可能与现在的职责大不相同。在未来，律师的职责不是裁定个人合约，而

是在一个竞争市场上生产智能合约模板。合约的卖点将是它们的质量、定制性、易用性如何。许多人将会针对不同事项创建合约，并将合约卖给其他人使用。所以，如果你制作了一个非常好的、具有不同功能的权益协议，那么就可收费许可别人使用。以智能合约管理遗嘱为例，如果你的所有资产都是比特币，用智能合约管理遗嘱的方式就可行。对于实体资产，智能资产也能解决这些问题。在尼克·萨博（Nick Saab）1994年的论文中，他预想到了智能资产，写道：“智能资产可能以将智能合约内置到物理实体的方式，被创造出来。”

智能资产的核心是控制所有权，对于在区块链上注册的数字资产，能够通过私钥来随时使用。这些新理念、新功能结合在一起会怎么样呢？以出租房屋为例，我们假设所有的门锁都是连接互联网的。当你为租房进行了一笔比特币交易时，你和我达成的智能合约将自动为你打开房门。你只需持有存储在智能手机中的钥匙就能进入房屋。当这些数字钥匙到期时，智能合约也将使得设置日期更加容易。

未来我们的房产、车库、门禁系统也许都会植入软硬件的识别设备，主人使用时，自动识别主人注册在区块链的数字身份即可，如同好莱坞科幻电影场景，让我们进入便捷的智能世界。

智能资产的一个典型例子是，当一个人偿还完全部的汽车贷款后，智能合约会自动将汽车从财务公司名下转让到个人名下（这个过程可能需要多个相关方的智能合约共同执行）。但如果贷款者不还款，智能合约将自动收回发动汽车的数字钥匙。

基于区块链的智能资产，让我们有机会构建一个无须信任的去中心化的资产管理系统。只要物权法能跟上智能资产的发展，通过在资产本身上记录所有权将极大地简化资产管理，大幅提高社会效率。

有执行力的合约

现行法律的本质是一种合约。它是由人（生活于某一社群的）和他们的领导者之间所缔结的，一种关于彼此该如何行动的共识。个体之间也存在着一些合约，这些合约可以理解作为一种私法，相应地，这种私法仅对合约的参与者生效。

例如，你和一个人订立合约，借给他一笔钱，但他最后毁约了，不打算还这笔钱。此时你多半会将对方告上法庭。令人欣慰的是，当初你和借款人把条款写了下来，订立了合约。但法律的制定者和合约的起草者们都必须面对一个不容忽视的挑战：在理想情况下，法律或者合约的内容应该是明确而没有歧义的，但现行的法律和合约都是由语句构成的，而语句则是出了名的充满歧义。因此，一直以来，现行的法律体系都存在着两个巨大的问题：首先，合约或法律

是由充满歧义的语句定义的；其次，强制执行合约或法律的代价非常大。而智能合约通过编程语言，满足触发条件即可自动执行，有望解决现行法律体系的这两大问题。当然如果你不是一名程序员的话，一开始就读懂合约可能要花点时间，但一旦学会如何阅读，这份合约绝对比现有的律师们起草的合约要通俗易懂得多。如果采用这种方式，简单的合约一般的用户就可以起草，特殊一点的合约可能需要稍微资深一点的专家起草（就像复杂的传统合约也需要专门的律师起草一样）。作为结果，我们得到的这份合约，完全消除了类似“我认为，你认为”的这种误解，缔约双方是否依法履约的不确定性也一并被消除。也就是说，代码写成的这份合约，既定义了合约内容，也保证了合约内容的执行。在本质上，这份合约真的就是一份不会毁约的合约，而这一点非常强大。

初期，智能合约会首先在涉及虚拟货币、网站、软件、数字内容、云服务等数字资产的领域生根发芽，因为针对数字资产的“强制执行”非常直接有效。但是，随着时间的推移，智能合约会逐步渗透到“现实世界”。比如，基于智能合约的某种租赁协议的汽车可以通过某种数字证书进行发动（而不是传统的车钥匙）。而如果这个数字证书不符合该租赁协议（例如证书到期），汽车就不会发动。

在一个私法和公法可以被完美地监督和执行的未来世界里，很多事情都变得可能。你可以设想一个当地法律都靠智能合约订立的小镇。在这个小镇上，新法的通过和针对既有法律的修正案都必须通过投票系统进行公开投票决议，而且这个投票系统也是由智能合约实现的。同时，镇上的居民也会非常清晰地意识到法律的执行和适用范围。你甚至可以想象一个不靠地理边界而是基于智能合约的法规和权益的国家，未来人们甚至可以自由选择最适合自己的虚拟国度。

从未来的角度看，今天现行的法律系统看起来就像茹毛饮血般原始。我们拥有连篇累牍的即使在法院看来也依然充满歧义的法律条文。同时，我们订立的合约充满了虚假的个人承诺和渺茫的兑付希望。因此，随着智能合约的出现，一种新的法律形式即将诞生。

区块链未来应用蓝图

我们来看看未来区块链技术会怎样影响我们的生活。

20年后的某一天，M国总统大选正在如火如荼地进行，你把智能手表调到投票界面，看了下选举人：今年好像没什么有特色的竞选人啊。李·查得？没意思，一个中规中矩的政治家，一直想把世界扭转回中心化的统治下。拜托，我选的总统是为人民服务的，不是来统治人民的。

于是你划到下一个：王·大卫？这个人好像挺耳熟，对了，之前好像是做金融的，听说他用区块链技术把之前的银行推翻后帮助大家建立了许多自己的“银行”。听起来感觉不错，但是我对金融不感兴趣，下一个。

看到个有意思的家伙，斯蒂芬·奇，他创造了一系列新的货币，希望能够颠覆目前各个阶级的统治。不错，就选这个，反正现在用的是区块链技术投票，投谁都不用怕被查水表了。

投完票后，你抬头看了下旁边的高楼大厦，广告牌里正在宣传OB——一家利用比特币进行交易的去中心化电商平台。该平台直接将用户与用户连接起来开展交易，OB实现了买卖双方的直接交易，而不需要借助中心化的平台。不同于之前相当于第三方的阿里巴巴，OB可以直接使交易双方在信任的基础上促成交易合作。由于去中心化、无组织管理，这意味着当用户在OB进行交易时，不需要支付额外费用、不会泄露档案、进行的任何交易也不会被审查。

前天在OB上买的纪念版比特币卖家说违规销售，不想卖就直接说嘛，OB上卖东西、买东西都是匿名的，又不是购买毒品什么乱七八糟的。

看了下时间，医院挂号马上要到时间了，得抓紧过去。你想起之前爷爷说他年轻的时候去看病，每次看完病都能收到一大堆乱七八糟的医疗短信，那会儿填单子的时候都不敢填自己的真实姓名，就是怕自己的身份信息给泄露出去了。现在有区块链技术提供可行的替代方案，在公开透明的同时也尊重保护了用户的隐私。集中的数据库和文件柜都不再是一个切实可行的选择。过去，由于内部失误，患者机密信息会被泄露。随着时间的推移，通过采用像区块链这样的创新技术，安全性和记录推移将得到改善。

晚上回到家，你通过智能手表发出一个指令，家里所有的东西又开始工作起来。你打开了计算机准备在论坛上逛一逛，论坛上又是一些关于中心化和去中心化的讨论，你与这些人激烈探讨起来，反正论坛也使用了区块链技术，不用担心信息被泄露出去。

以上是对未来世界里一个普通人日常生活的设想。区块链的核心思想是去中心化，在人与

人、点与点、端与端之间不相识的时候，可以通过计算机技术（区块链技术）建立信任，节约了大量的成本，提高了办事的效率。区块链的特性是它不会被伪造，信息高度透明。区块链的这两个特性被应用得比较广。

区块链不仅会重塑货币市场、支付系统、金融服务及经济形态的方方面面，而且会改变人类生活的每个领域。区块链技术能够从根本上成为让组织形态减少摩擦并且提高效率的新方案。区块链去中心化的特性与整个网络的流动性能将所有人连接在一起，无须中间人或身份信息交流中心的参与就可以实现所有权和信息的信息处理；提供了一种通用技术和全球化的解决方案，自动化地实现物理资源和人力资源的分配，解放了过去由人力来完成的各种协调和确认。也许以后所有人类活动都可以通过区块链来协调。

为什么区块链会率先颠覆金融领域

由于区块链技术最早来自比特币，所以最早接触和应用的大多是金融机构。现在传统的金融行业中涉足最多的是银行、证券交易和登记的环节。目前医疗、供应链、物联网、游戏、政务、公证、社交、人工智能等领域的应用多处于初级或概念设立阶段。据科技行业并购咨询机构Magister Advisors估计，到2017年，银行投入区块链开发的经费将超过10亿美元，是所有企业软件板块发展速度最快的。

2015年9月建立的初创公司R3 CEV发起R3区块链联盟，至今已吸引了包括富国银行、花旗银行、德意志银行、汇丰银行、摩根士丹利、加拿大皇家银行、澳大利亚国民银行和法国兴业银行等43家银行巨头参与，着手为区块链技术在银行业的使用制定行业标准和协议。纳斯达克在2015年12月30日也完成了基于区块链平台的首个证券交易，对于全球金融市场的去中心化有着里程碑式的意义。将来会有越来越多的区块链股票交易尝试。

除了为金融交易带来高透明度、高安全性、降低欺诈风险之外，区块链技术还能够帮助提高效率 and 减少开支。2015年6月，西班牙桑坦德银行发布的研究报告提出，截至2022年，区块链技术通过减少跨境支付、证券交易以及合规中的成本开支，每年能为银行业节省150亿~200亿美元。

国内首个区块链项目“小蚁”的创始人达鸿飞认为，“区块链技术普及后对银行业的影响是变革性的，金融的底层基础架构会发生变化，原有的一些角色将来可能就不再需要了，有可能会有一些新的角色，所以对底层会造成很大的变化”。比如金融业中有一些登记结算机构，如A股市场里的中国证券登记结算有限公司，债券市场的中央国债登记结算有限责任公司，这一类机构完全可以被区块链技术取代。澳大利亚证券交易所就正在与一个叫数字资产控股（DAH）

的区块链初创公司合作，由DAH提供技术为他们建造一个基于区块链技术的清算和结算系统。

传统金融互联网化的意义在于减少中间环节、降低交易成本、扩大金融服务范围、提高金融服务质量等。而区块链技术的嵌入则可能会将互联网金融的意义深化。其中一个重要方面是，可通过程序化记录、储存、传递、核实、分析信息数据，从而形成信用。相较于传统的信用形成方式，区块链可省去大量人力成本、中介成本，所记录的信用信息更为完整、难以造假。

举例来说，当我们申请贷款时，需要提供相应的信用信息，这就需要依靠银行、保险或征信机构所记录的相应信息数据。但其中存在着信息不完整、数据不准确、使用成本高等问题，而区块链的用处在于依靠程序算法自动记录海量信息，并存储在区块链网络的每一台电脑上，信息透明、篡改难度高、使用成本低。因此，申请贷款时不再依赖银行、征信公司等中介机构提供信用证明，贷款机构通过调取区块链的相应信息数据即可。

在审计方面，公司不需要招聘专门的审计人员来公司内部审核账本，所有交易都可以集中记录储存在内部的区块链。由于区块链具有不可逆性和时间戳功能，会计事务所等外部审计人员和监管机构通过跟踪这些区块链可以实时监控公司账本，同时机构可以借此大幅减少对于审计员审核金融交易的依赖，将审计业务变得更有效率。

R3 CEV组建区块链联盟的目的就是要做一个全球的去中心化的实时结算清算系统。目前，如果要汇款到国外，即变汇是需要通过SWIFT（环球同业银行金融电讯协会）系统的，这个过程往往需要t+1或者t+2，甚至t+3。如果使用区块链技术，理论上就可以实现实时结算和清算，相当于一个全球的支付宝体系。在这种理想状况下，银行是获利最大的，因为他们不用通过SWIFT系统，首先是极大地降低了成本，同时由于实时结算，也减少了来自对手的风险。这种全球的去中心化的实时结算清算系统能够让全球的金融体量上一个新的台阶。

在中国的区块链创业圈中，一位名为Certchain的全自动鉴证服务项目致力于不依靠第三方介入，以数学算法免费对信息数据的真实存在提供证明，其官网介绍称：“对任意文件和任何信息，以去中心化的方式，用纯粹的数学算法的方式提供匿名且安全的存在证明，并可以根据用户的需求，无须任何第三方介入，能够便捷和以极低成本证明某个人对任意类型文件的所有权。”

“区块链本质上就是交易各方信任机制建设的一个完美的数学解决方案。”中国万向控股有限公司副董事长兼执行董事，万向区块链实验室发起人肖风认为，“一是用纯数学算法来建立各方的信任关系；二是交易各方信任关系的建立完全不需要借助第三方；三是建立信任关系的成本几乎为零。这也正是我预言的区块链将帮助达成互联网金融终极模式的核心所在。”

以区块链为基础，再加以辅助方法可在互联网上建立智能合约机制，用程序代替合同，当

约定的日期、条件一旦达成，网络自动执行合约，金融活动由交换数据变成交换代码。

区块链技术将成为下一代数据库架构

在互联网诞生初期，数据库主要的类型是关系型数据库，这是一种采用了关系模型来组织数据的数据库。1970年由IBM的研究员E. F. Codd（埃德加·弗兰克·科德）博士首先提出，在之后的几十年中，关系模型的概念得到了充分发展并逐渐成为数据库结构的主流模型。简单来说，关系模型指的就是二维表格模型，而一个关系型数据库就是由二维表及其之间的联系所组成的一个数据组织。

随着互联网web2.0网站的兴起，传统的关系数据库在应付web2.0网站，特别是超大规模和高并发的SNS类型的web2.0纯动态网站时已经显得力不从心，暴露了很多难以克服的问题，而NoSQL的数据库则由于其本身的特点得到了非常迅速的发展。NoSQL泛指非关系型的数据库，它的产生就是为了解决大规模数据集合多重数据种类带来的挑战，尤其是大数据应用难题。

谷歌（Google）公司的三篇著名论文（GFS，Bigtable，MapReduce）奠定了谷歌大数据的基础，而谷歌的PageRank算法实现了当时几乎最先进的数据搜索算法。PageRank通过网络浩瀚的超链接关系来确定一个页面的等级。Google把从A页面到B页面的链接解释为A页面给B页面投票。Google根据投票来源（甚至来源的来源，即链接到A页面的页面）和投票目标的等级来决定新的等级。简单地说，一个高等级的页面可以使其他低等级页面的等级提升。而这个技术正是数据第二阶段，通过复杂的设计网络和算法进行重新整理和归纳，让原本看似并无关联的数据成为可以分级分类的高质量数据，让大数据和复杂网络模型成为可能。

但是构建在这之上的大数据最大的问题就是无法解决信任问题。因为互联网将使全球的互动越来越紧密，伴随而来的就是巨大的信任鸿沟。目前现有的主流数据库技术架构都是私密且中心化的，在这个架构上永远无法解决价值转移和互信问题。所以区块链技术将成为下一代数据库架构，通过去中心化技术，将在大数据的基础上解决全球互信这个巨大的难题。通俗来说，该技术可被理解为全体参与记账的技术，过去人们使用一台中心化的服务器记账，而在区块链技术系统中，每个人都可以参与记账，并共同鉴定记录的真伪。

区块链可以和大数据连接，大数据预测分析可以和自动执行的智能合约完美结合。区块链技术加入经济支付层面，作为量化工具，海量自动执行的任务会解放大量的人类生产力。区块链也会促进大数据向下一个数量级发展。通过这项技术，即使没有中立的第三方机构，互不信任的双方也能实现合作。简而言之，区块链类似一台“创造信任的机器”。

区块链技术作为一种特定分布式存取数据技术，通过网络中多个参与计算的节点共同参与

数据的计算和记录，并且互相验证其信息的有效性（防伪）。从这一点来看，区块链技术也是一种特定的数据库技术。这种数据库将会实现Melanie Swan所说的第三种数据类型，即能够获得以基于全网共识为基础的数据可信性。从目前来看，我们的大数据还处于非常基础的阶段，但是当进入区块链数据库阶段时，将进入真正的强信任背书的大数据时代，这里面的所有数据都将获得坚不可摧的质量。

分布式的区块链开辟了各种可能性，例如：分布式投票（如Agora），选民可使用加密货币代表他们的选票，而拥有最多额度账户的候选人将由此胜出；分布式域名注册（DNS，如Namecoin），将根据加密货币的模式来实现独立的ICANN的工作；分布式存储（例如MaidSafe和Storj），无须信任的节点在一起工作（使用加密货币作为支付手段）来交换存储空间和带宽；甚至是分布式的、点对点的异步消息传递平台，例如BitMessage（比特信）和Twitter（推特）。

区块链将如何颠覆我们的生活

想象这样的一个世界——你可以用你的手机参与选举，可以几个小时就买套房子，或者压根儿就不存在现金这回事。这正是区块链为我们描绘的未来。

在西弗吉尼亚大学，学生会正在考虑要不要用基于区块链技术的投票平台来进行学校选举。如果运用这样的平台，学生们就能用移动设备来投票，而由于投票结果会被计入公共系统，因此投票是完全安全的。一名支持这种方式的学生解释到，“大家的投票绝不可能被我们——即程序员、学校管理员或学生修改、删除”。相信在不久的将来，这种安全的投票形式将会被运用到更为重要的地方——总统大选。

未来区块链会应用于任何领域，给人类生活带来极大影响。区块链应用项目大致分为：存在性证明、智能合约、物联网、身份验证、预测市场、资产交易、电子商务、社交通讯、文件存储、数据API（应用程序编程接口）等。

1. 医疗去中心化

医疗方面，区块链最主要的应用是对个人医疗记录的保存，可以理解为区块链上的电子病历。目前病历是掌握在医院手上的，患者自己并不掌握，所以病人就没有办法获得自己的医疗记录和病史情况，就像银行的账看不到过往的交易记录一样，这对未来的就医会造成很大的困扰。但现在如果可以用区块链技术来进行保存，就有了个人医疗的历史数据，未来看病或对自己的健康做规划就有数据可供使用，而这个数据真正的掌握者是患者自己，而不是某个医院或第三方机构。另外，这些数据有很强的隐私性，使用区块链技术也有助于保护患者隐私。

这种应用具有去中心化的特性，更具开放性，用户也更有自主性。它所实现的是一种新的组织信息的形态，每个人都掌握自己的信息，而不需要像过去那样把信息托管给某一个机构来保管。

2. 智能锁

德国一个初创公司Slock.it想做一个基于区块链技术的智能锁，并将锁连接到互联网，通过区块链上的智能合约对其进行控制。任何一个控制锁的人都可以发放一把或多把私钥，并对私钥进行复杂的定制，设定锁什么时候启用、具体什么时候开等。通过这种方式，共享经济能够被进一步去中心化，将任何能被锁起来的東西轻易租赁、分享和出售。Slock.it的概念更是超越了为Airbnb（空中食宿）用户服务的范畴，想要进一步颠覆这种共享经济，让使用者能够直接向一把锁进行支付，然后打开；出租者也可以随时更换私钥的定制，让整个体验更为方便、安全。人们也可以通过使用这一技术进行自行车、密码柜的租赁等，甚至让他人自家门口给车充电，然后收取费用等。

3. 去中心化域名系统

区块链可提供DNS系统替代方案，不被公司控制。它能够让全世界任何人自由地在互联网上发布信息。

4. 数字艺术：区块链认证服务

数字艺术是区块链加密技术能提供颠覆性创新的另一个舞台。数字艺术在区块链行业的主要应用是指，利用区块链技术来注册任何形式的知识产权，或将鉴证服务变得更加普遍，如合同公证。数字艺术还可以通过区块链来保护在线图片、照片或数字艺术作品这些数字资产的知识产权。

5. 区块链政府

区块链以去中心化、个性化、便宜高效的特点提供传统服务，实现全新的、不同的政府管理模式和服务。充分利用区块链优势，能让政府工作更高效，进而获得民众的信赖。

区块链能利用其公开永久保存数据的优势——共识驱动、公开审计、全球性、永久性——保存所有社会档案、记录和历史，供未来使用，成为全球性的数据库。这将成为区块链政府服务的基石。通过区块链技术重新配置公共资源、提高政府效率、节约成本、让财政惠及更多人、提高民众基本收入水平、促进平等、提高民众政治参与度，最终过渡到自治的经济形态。

不妨再设想一下更加久远的未来：当区块链所代表的思维范式，这种鸟群般的分布式协作、去中心化的模型，不仅仅应用于货币、资产的合约交易，不只是限定在可设定、可编程的

物与物之间，不仅仅是普通的物理实体的万物互联，而是直接作用于我们的大脑、神经元与认知，当人类大脑与计算机接口技术，配合区块链网络共同展开，当人类与机器人记忆的提取、交易、存储得以实现，当知识、灵感与创意的交互链条有序地形成，并不断演进，那又将是怎样的爆发式增长，何等恢宏壮丽的景象。

6. 在线音乐

许多音乐人正选择区块链技术来提升在线音乐分享的公平性。Billboard（公告牌、美国音乐杂志）报道，目前有两家公司正通过直接付款给艺术家和利用智能合同来自动解决许可问题。在区块链音乐流平台上，用户可以直接付款给艺术家，而无须中间人插手。除了媒体音乐，还有人预想，将智能合同作为歌曲清单的自主大脑，能够更好地将歌曲背后的艺术家和创作者分类。

7. 汽车租赁和销售

Visa和DocuSign公司宣布了一项合作计划，利用区块链技术为汽车租赁打造特定解决方案，以后汽车租赁只要“点、签、开”三步即可完成。具体操作是：顾客选择想要租赁的汽车，这笔交易就会上传到区块链的公共账户；然后，顾客在驾驶座签署一份租赁协议和保险协议，区块链便会实时将信息上传。不难想象，这种租赁模式或许也将应用于汽车销售和汽车登记领域。

8. 全球公共卫生及慈善捐赠

比特币可以为埃博拉等传染病危机提供高效、直接、有针对性的资金援助。传统银行资金流动过程会妨碍危机处理过程中对资金的紧迫需求，而比特币可以迅速把资金传递到一个公开且可以审计和跟踪的地址。未来慈善捐赠网站可以透明地接受比特币捐赠，筹集大量善款开展项目。

9. 区块链基因测序

当前公民获取个人基因数据有两个问题：第一，法律法规对于个人获取基因数据的限制；第二，基因测序需要大量计算资源，高昂费用限制了产业进程。区块链测序则解决了这两个问题：通过全球分布的计算资源，低成本地完成测序服务，并用私钥保存测序数据规避了法律问题。有了数据，如果发现有潜在的高血压、老年痴呆症，可以提前改变生活习惯来减少其发生概率。相信在不远的将来，随着区块链基因测序技术的成熟，面向大众消费者的基因测序服务将得到普及。

区块链应用到大数据领域，使其进入下一个数量级，迎来真正的大数据时代，基因测序就是推进大数据的一个典型案例。

10. 区块链智能城市

生活在基于区块链的智能城市，我们可以为自己制造的麻烦付费：发生交通事故造成拥堵，可以支付给过往车辆延误费用，促进社会向自律、高效自治的方向发展。我们还可以公开透明地为好的服务、好的学校支付费用。

11. 区块链透明助学

区块链的智能合约有无数用途，智能文化合约就是其中一种。如果有人给孩子提供上学资助，可以通过智能合约自动确认学习进度，满足学习合约后，自动触发后续资金拨付给下一个学习模块。区块链学习合约能够使学习者和资助者之间完全以点对点方式进行协调，公开透明，对双方都是正向激励。学习合约将为慈善资助带来革命性的突破。

12. 数字身份验证

现在很多网站使用中心化的第三方登录，比如QQ登录、微博登录。那么未来，我们也许就会使用区块链技术提供的去中心化第三方服务登录，可以用姓名、地址或二维码登录，且和手机绑定，可以自由畅游网络世界。在电商网站购买时，也不需要烦琐的绑定银行卡就可转接到支付宝、微信等操作，直接用数字钱包一键购买。

13. 区块链身份认证

区块链具有人人可以查阅的特性，每个人都可以在任何一个有网络的地方，查询区块信息，高度透明的特性也让区块链充满魅力。不妨这样设想，在以后身份证和户口本基本不需要了，因为每个身份信息都可以写入区块链里，当需要验证信息的时候，只需要查阅就可以找到。无论是追拿逃犯还是证明“你妈是你妈”都不再是问题。

14. 区块链婚姻

区块链婚姻是区块链作为公开档案信息库的一个尝试，如果以后能得到广泛推广和认可，会带来很多好处：更加透明、公平、自由，能解决重婚、隐婚等各种情况，并通过智能合约来改善赡养老人、生儿育女、购买房产等生活事宜。

15. 学历证书

加州软件技巧项目Holbertson School宣布，它将利用区块链技术来鉴定学历证书。此举将确保Holbertson School的学生在课程认定上的真实性。如果更多的学校采用这种透明的学历证书和成绩单，那么学术界的腐败将大幅减少，更不用说省去的人工核验时间和纸质文件成本了。

16. 预测

区块链技术或将撼动整个研究、分析、咨询和预测行业。在线众筹平台Augur希望能在去中心化的预测平台赚取利润。这家公司称，它将提供一种类似博彩互换的服务。整个过程将被去中心化，Augur平台不仅会给用户提供体育和股票博彩服务，还将提供选举和自然灾害博彩服务。这个想法实际上是超越了体育博彩的范畴，创造了一个“预测市场”。

17. 网络安全

虽然区块链的系统是公开的，但其核验、发送等数据交流过程却采用了先进的加密技术。这种技术不仅确保了数据的来源正确，也确保了数据在中间过程不被人拦截、更改。如果区块链技术的应用更为广泛，那么其遭受黑客袭击的概率也会下降，区块链系统之所以能降低传统网络安全风险就是因为它解除了对中间人的需求。省去中间人不仅降低了黑客袭击的潜在安全风险，也减少了腐败产生的可能。

18. 人工智能区块链

区块链让智能设备在设定的时间进行自检，会让管理人员回到设备出故障的时间点去确定究竟什么地方出了错。应用区块链技术可以远程实施人工智能软件解决方案。如果一个设备有多个使用者，人工智能区块链也可帮助提高安全性，区块链会让使用各方共同约定设备状态，基于智能合约中的语言编码做决定。

各国政府的态度——从比特币到区块链

区块链从本质上来说可以看作是一个去中心化的数据库，其本身作为一种技术而存在。如果我们把区块链技术比喻成花盆里的土，那么比特币则是在花盆里生长的一株花；比特币是在区块链的基础上所诞生的一种数字货币，区块链则是比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

区块链1.0：游走在法律边缘的比特币

比特币去中心化的特点注定它不能被某一个国家或者团体所掌控，这对于某些本国货币强势的国家来说是不被接受的：世界上最赚钱的事情就是印刷货币，经济强国可以通过印刷货币获得大量的财富，并且这是一个可以控制、牢牢掌握在自己手里的金融工具，所有外交、军事、对外发展等活动都可以在某些情况下印证国家对于本国货币地位提升的重要性。而比特币的出现却让这些经济强国出现了危机：比特币可以被世界上任何一个人“印刷出来”，经济强国最可控的“生意”——印刷货币，受到了挑战。未来如果比特币成为世界主流货币，那么世界的货币体系将会发生改变，经济强国再也无法倚仗自己的印钞机掠夺财富，由此会导致权威地位的下降，这对某些国家来说是不可接受的。

而对于其他较为落后的国家，比特币的出现也许是一个弯道超车的机会。在没有出现较大的世界性危机之前，落后的国家很难在现有的货币体系中为自己获得更多的利益。不确定性在某一方面同时也意味着机会，每一次经济体系的改革都会重新诞生一批强国，而比特币的出现则让它们看见了希望。

在比特币诞生初期，各国政府对其态度各不相同。

1. 美国

美国财政部下属的金融犯罪执法网络出台了一份针对比特币等虚拟货币业务的指导性文件——《金融犯罪执法网络法规在个人管理、交换和使用虚拟货币中的应用》。该文件认为，比特币是一种典型的虚拟货币，不具备实际货币的全部属性和法定货币地位。2014年初，美国联邦税务局发布通告称比特币及其他虚拟货币属于财产而不是货币，比特币的“挖矿”、买卖和使用行为均应适用相关税务规则，进行纳税申报。

2. 中国

中国人民银行联合相关部委下发的《关于防范比特币风险的通知》认为，比特币不是由国家发行的，不具有法偿性与强制性等货币属性，并不是真正意义上的货币，不能且不应作为货币在市场上流通使用。

3. 韩国

拒绝承认比特币的货币地位，比特币不是真正的投资，不会对比特币征收资本所得税，因为这将会增加虚拟货币的合法性。

4. 荷兰

发布声明警告比特币风险，质疑比特币存储无法保障，不是由政府 and 央行发行，导致比特币价格波动剧烈。

5. 德国

2013年8月，德国承认比特币的合法地位，已经纳入国家的监管体系。德国也成为世界首个承认比特币合法地位的国家。德国政府表示，比特币可以当作私人货币和货币单位，比特币个人使用一年内免税，但是进行商业用途要征税。德国金融监管局认为比特币是用来交换真实经济品或服务在物物交换俱乐部（barter-club）、私人集市或其他支付系统流通的价值代币。因此，比特币在德国实际上被定义为一种商品。这类似于最近一些政府决定把比特币捐赠当作实物捐赠（如捐赠食品和物资）的做法。目前德国的比特币政策相对明朗，德国本土的比特币交易平台bitcoin.de也已经与Fidor银行展开合作。

6. 加拿大

承认比特币的“货币地位”。2013年12月世界首个比特币ATM机已经在温哥华投入使用，这台机器安放在一个咖啡厅里。目前，这台机器上的交易额已经取得很好的成绩。很多美国本土的比特币创业者，由于国内不同州的法律监管问题，选择搬迁到加拿大创业。

7. 法国

认为比特币交易并不违法。法国金融情报机构（TRACFIN，一个反洗钱机构）公布了2011年度报告，描述了各种形式的虚拟货币洗钱以及位于全球众多金融避难港的不法公司。例如，银行业人士利用没有法定价值的虚拟货币进行非法活动。尽管报告的焦点是反洗钱，但报告内容中所透露出来的对比特币的使用案例等于在事实上承认了比特币使用的完全合法性，即利用比特币避开欧元区和使用美元的非欧元区的外汇兑换和转账的相关费用。对于比特币价格的波动，法国政府则警告用户谨慎投资比特币。

8. 泰国

泰国外汇管理和政策部的高官表示，由于缺乏适用的法律和资本管制措施，加之比特币跨越多种金融业务，因此下述比特币活动在泰国都被视为非法：买卖比特币、用比特币买卖任何商品或服务、与泰国境外的任何人存在比特币的往来。泰国比特币创业公司Bitcoin Co表示，由于泰国央行封杀了比特币，因此该公司将停止所有业务。泰国成为全球范围内封杀比特币的首个国家。

9. 印度

将继续关注比特币的发展，目前不会进行监管。相关机构表示，虚拟货币给监管、法律以及运营风险带来了挑战。

10. 以色列

目前尚未承认比特币为官方货币，但是政府正在考虑对比特币的盈利征税。以色列的比特币社区也相对活跃。

后比特币的2.0时代

1. 俄罗斯：又爱又恨

俄罗斯对比特币和区块链技术的立场堪称反差巨大，很值得研究。尽管俄罗斯一向不看好比特币，对比特币所用的区块链技术却充满热情。

俄罗斯中央银行组建了分析、评估、应用新兴金融科技可能性的工作小组，旨在分析金融市场中的先进技术和创新技术，几大首要研究对象包括区块链技术、移动技术、支付技术等领域。

俄罗斯一向对比特币采取强硬态度，但与财政部曾起草法案禁止使用包括比特币在内的各类货币替代品相较而言，情况已经有所改变。2016年初，在财政机构和企业的几次会议之后，俄罗斯央行很可能会开始考虑合法化比特币和监管比特币交易，尤其是P2P交易及个人业务托管。俄罗斯境内现共有20万名加密货币用户，居全球第五，因此如果上述提案通过并开始实施，虚拟货币在俄罗斯的发展将会更进一步。

2. 日本：或视比特币为现金

比特币在日本的发展历程十分有趣。日本金融监管人员考虑将比特币等虚拟货币视为与现

金等价的货币，此举将强化消费者保护机制，铺设一条虚拟经济增长的发展道路。在日本，比特币现在仍被视为物品，无法受到与其他同类产品相同的待遇。

据日经新闻（Nikkei）报道，日本金融厅（FSA）正在考虑修订法案，将比特币等虚拟货币合法化，使电子币“实现货币功能”。此举将使一些虚拟货币交易企业受到管制，虚拟货币以更加安全的模式推广。

3. 澳大利亚：将影响经济和政治领域

澳大利亚证券和投资委员会主席Greg Medcraft（格雷格·麦德克夫特）在演说中提及区块链。他说：“这项技术具有从根本上改变市场和金融系统的潜力。区块链对于我们的监管方式有着深远的指导意义。”澳大利亚证券交易所（ASX）早已与加密货币公司Digital Asset Holdings建立了合作关系，将利用区块链技术为澳大利亚证券市场研发解决方案。2016年2月，位于墨尔本的比特币挖掘企业Bitcoin Group在澳大利亚股票交易所上市，完成首次公开募股，集资420万美元。这是首例比特币挖掘企业公开募股。

区块链也应用于政治中。一个新政党Flux正在试图利用区块链技术改写政治通货制度。Flux运用区块链技术推出现代投票系统，使投票透明化、记录不可更改化、在线投票便利化。2016年1月，Flux向澳大利亚选举委员会提交了申请报告，计划通过这一系统选出六名议员。Flux给自己的定位是重新分配政权的开路者。一旦有Flux内的候选人当选，Flux即成为选民可直接影响议会的门户。截至目前，Flux网站共有1238名注册用户。

4. 韩国：将引进区块链

韩国证券期货交易所（KRX）运用区块链技术，已经启动建立场外交易平台的初期计划。这一新平台将把场外交易市场（OTC）的买家和卖家聚集到一起，在此寻找交易伙伴，降低参与成本，从而促进交易的进行。

5. 迪拜：建立全球区块链委员会

为推进创新发展，在全球范围内采用新技术，迪拜未来博物馆基金会近日宣布建立全球区块链委员会。迪拜未来博物馆基金会CEO Al Aleeli（阿尔·艾莉）表示，“2015年通过区块链平台实现的交易增长了56%，这一显著增长意味着在相关领域优化运用这项技术的巨大机遇”。他还表示，在今后4年内，区块链全球投资额可达3000亿美元。全球区块链委员会将继续探索运用区块链技术的最佳方式，同时研究其优缺点，推进区块链和数字货币的发展。

6. 欧洲议会：发布虚拟货币报告

欧洲议会新起草的一项虚拟货币报告强调，虚拟货币与区块链技术可大幅降低交易中支

付、资金转移等成本，对消费者福利和经济发展做出重要贡献；同时提高支付系统的速度和弹性，可跟踪记录交易，以防不法行为。

这份报告提出组建由委员会领导的分类账簿技术特别工作组，以此激励重要的技术专家和监管专业人员支持相关行动者（包括欧盟和成员国），确保对新的机遇和挑战做出及时的、通晓各方的回应。

同时，欧洲中央银行对新技术持开放态度，表示欧洲央行计划对区块链和分类账簿技术与支付、证券托管以及抵押等银行业务的相关性进行评估。

当区块链开始吸引高科技公司、跨国金融机构和知名创投基金的投资热情时，各个国家和地区央行也纷纷针对虚拟货币与区块链技术对金融系统和监管思维的潜在影响进行研究并发表看法。

各国政府对比特币的监管

比特币的问题出现在监管上。事实上，由于数字货币拥有无国界的网络性质，以及无法具体到某一个国家的发行人（或者说每个人都有可能是其发行人），这对于任何一个国家主管部门的监管能力都是很大的挑战（虽然其他可识别的第三方供应商可能会更容易被监管）。

比特币的交易全部都在网络上进行，基本不受各个国家的影响，其所带来的好处是，可以使交易变得便捷、快速、廉价。例如，一家在美国做跨国生意的企业需要支付一笔50000美元的货款给中国企业，在没有比特币的情况下，他需要先进行跨国转账，中国企业在收到这笔货款后也需要去银行兑换成人民币，其中所花费的转账手续费、兑换手续费都是非常高的，并且这一个过程所耗费的时间非常长，但是比特币正在慢慢地改变这种现状。美国企业现在只要用50000美元在交易平台上购买等额的比特币，然后把比特币转到中国企业的账户中，中国企业在收到比特币的时候在交易平台上卖出去就行了。为了防范时间差所带来的比特币贬值风险，中国企业只要在平台上购买一份等值的看空合约就可以预防其中的风险，相对于跨国转账的手续费来说支付给交易平台的手续费实在是微不足道。

但是国家在这一笔交易中所能起到的监管作用就变得非常小，国家只能对其国内的交易平台进行监控，而对交易本身存在非常大的监管漏洞。在2014年，反洗钱金融行动特别工作组（FATF）发表了一个关于数字货币问题的大篇幅报告，指出“可兑换法币或用其他可兑换的虚拟货币更容易卷入洗钱和恐怖融资活动”，而最近FATF面向虚拟货币支付产品和服务发布了风险管理办法的指导意见，提出面对类似的产品和服务，根据其功能和风险状况建立跨区域的指导，对于强化国际反洗钱/反恐融资标准的效力是至关重要的。

表2-1 各个国家对于比特币的监管

主要手段	监管类型/国家示例
信息/道德劝说	公共警告 投资方/买家信息 研究报告
具体利益相关者监管	
现有监管解读	监管实施基于对现有框架（比如税法处理）如何应用于数字货币或数字货币中介机构的解读。例如：美国
总体监管	涵盖所有三个方面的专门法规（消费者权益保障，针对不同利益相关者的审慎的组织规则和支付系统的具体操作规则）
禁止	禁止比特币零售交易（或限制交易额） 禁止零售商接受数字货币付款 禁止基于数字货币的金融工具。例如：中国和比利时 封杀数字货币交易所 禁止银行间进行比特币交易。例如：中国和墨西哥

区块链技术可以被用于创造更多的集中式数字货币

世界各地越来越多的央行官员开始建议区块链技术可以被用于创造更多的集中式数字货币。

2016年2月，中国人民银行行长周小川在接受财新周刊专访时表示，“区块链技术是一项可选的技术”，人民银行也部署了重要力量研究探讨区块链应用技术，但是“到目前为止，区块链占用资源还是太多，不管是计算资源还是存储资源，应对不了现在的交易规模，未来能不能解决，还要看”。

2016年3月，英国央行分管货币政策的副总裁本·布罗德本特（Ben Broadbent）在伦敦政治经济学院演讲时提出，如果区块链技术继续发展，确实可能实现价值转移与登记无须经由某个具有公信力的第三方机构（如央行）来处理。严格来讲，央行是业务非常单纯的银行，主要职能是管理商业银行存在中央银行的储备资产，即“中央银行货币”（Central Bank Money），也就是中央银行的债券或央行本票。一般人对中央银行货币最熟悉的形式是在市面流通的现钞。如果民营企业者利用区块链技术平台大规模推广数字货币，那么央行最有效的反制措施就是尽可能地增加中央银行货币的流通，扩大直接向央行拆借的金融与非金融机构范畴，甚至让所有个人都在央行直接开户，并立法禁止使用现钞与硬币。这样的极端情境，在理论上无须区块链技术也能实现，但区块链技术能让事情更简单。

也就是说，国营的央行数字货币与民营的银行数字货币或许都基于相同技术，但其目的与使用情境可能大相径庭。央行账户越接近一般商业银行账户，央行数字货币就越能为人民服务，在市场上就越有竞争力，甚至会出现逆周期性的特征：当出现金融危机时，存款可能会从商业银行账户流向中央银行账户。布罗德本特认为，这个现象可能会让金融体系更安全。

目前各国政府和央行都还没有正式开始使用区块链技术，只是都在考察它的可行性方案，包括英国政府发布了一份80多页的报告，专门探讨其在各领域的可行性。英国目前的实时全额结算系统（RTGS）还不稳定，在2014年10月12日崩溃了9个小时，英国政府一直希望找到一套更稳定的解决办法，所以正在考察区块链的系统。目前的状态是还未投入实际使用，而是在研究发行数字货币RSCoin的方案中。

根据荷兰银行于2016年3月16日发表的一份最新年度报告所透露的信息，荷兰央行正在致力于开发一种被称为“DNBCoin”的内部区块链原型。荷兰央行表示，区块链技术可能会对银行现有的收入模式和银行监察系统产生影响。通过新的数字货币交换方式，将有可能为银行创造新的收益，也可能降低成本，并对荷兰央行的金融监管能力产生影响。但这也尚处于研究开发阶段。

各国政府态度开始出现变化。受到比特币底层技术区块链的吸引，花旗银行、高盛集团、巴莱克银行、摩根大通、苏格兰皇家银行和汇丰银行等银行业巨头也都加入了全球银行业区块链协议。该行业标准有望像如今的SWIFT一样，成为未来国际支付的标准。

商业银行基于区块链的应用领域

目前商业银行基于区块链的应用领域主要有：一是点对点交易，如基于P2P的跨境支付和汇款，贸易结算以及证券、期货、金融衍生品合约的买卖等；二是登记，区块链具有可信、可追溯的特点，因此可作为可靠的数据库来记录各种信息，如运用在存储反洗钱客户身份资料及交易记录上；三是确权，如土地所有权、股权等合约或财产的真实性验证和转移等；四是智能管理，即利用“智能合同”自动检测是否具备生效的各种环境，一旦满足了预先设定的程序，合同会得到自动处理，比如自动付息、分红等。

除了R3 CEV，国际上许多大型银行也以各种形式在区块链领域开展一系列探索，归纳来看有三种途径：一是商业银行成立内部的区块链实验室。比如花旗银行、瑞银、纽约梅隆银行等已相继成立研发实验室，重点围绕支付、数字货币和结算模式等方面测试区块链的应用，有的还扩大到其员工内部系统中测试。二是投资金融科技初创公司。2015年以来，许多跨国大型金融集团纷纷以创投形式进入区块链领域，比如高盛联手其他投资公司向比特币公司Circle注资

5000万美元，西班牙对外银行通过旗下子公司以股权创投方式参与了Coinbase的C轮融资等。三是与初创公司合作。例如巴克莱银行在技术孵化和加速器项目中与区块链初创公司合作，澳大利亚联邦银行和开源软件Ripple合作组队，创建了一个在其子公司之间互相支付转账的区块链系统等。

远在美国硅谷的创业者们聚焦于存储和应用，诞生了一批专注于比特币应用和区块链技术的创业企业，它们离普通用户更近：商业支付、跨境结算让数字货币超越技术层面的协议，真正具有了货币的属性，例如OKLink用区块链技术为金融机构和个人构建出一个快速、高效、安全的全球化金融网络。更值得称许的是，越来越多的创业者尝试在产业链最上游的区块链、数据挖掘等领域做基础设施层面的创新。

第三章

区块链率先敲开金融的大门

从贝壳到数字货币

从以物易物到以牛羊、布帛或者贝壳作为交换媒介，传递的是基于信任的生活理念。在人类漫长的关于货币的求索中，货币落脚在金属上，黄金承载了人类关于货币的记忆，而贝壳和布帛不过是货币的“脚注”。纸币是最原始的信用货币，随着科技的进步，货币的形式也更加丰富多彩，电子货币开始走入人们的视野。2009年，比特币横空出世，它是一串密码、一个数值，构筑了一个跨越时间、空间和国界的信任体系。

“二战”后，以美国为主导的“布雷顿森林体系”建立，美元确立了霸主地位。美元如一匹脱缰的野马，撒到了世界各地，尽管“布雷顿森林体系”在20世纪70年代就已经落幕，但是美元的主导地位并未改变。创造超主权储备货币一直是一个古老且悬而未决的问题。以比特币为代表的数字货币的崛起，已经引起了IMF以及各国央行的关注，为超主权货币提供了无限的想象空间。

那么，货币的实质是什么？为什么说黄金是天然的货币，而现行的货币体系为什么需要超主权货币去拯救呢？

货币的演变

1. 货币和货币体系

货币自身的发展主要有两条源流：一条是货币形式的演变；一条是货币职能的发展。从货币的形式上看，迄今为止，大致经历了“实物货币—金属货币—信用货币—电子货币”几个阶段。从总的趋势看，货币形式随着商品生产流通的发展、经济发展程度的提高，不断从低级向高级演变。这一演变大致分为四个阶段。

第一个阶段：一般价值形式转化为货币形式后，有一个漫长的实物货币形式占主导的时期。贝壳、布帛、牛羊等都充当过货币。

实物货币之所以随着商品经济的发展逐渐退出货币历史舞台，根本原因在于实物货币具有难以消除的缺陷。它们或体积笨重、不便携带；或质地不匀、难以分割；或容易腐烂、不易储存；或大小不一，难以比较。随着商品交换和贸易的发展，实物货币被金属货币所替代也就不足为奇。

第二个阶段：实物货币向金属货币转化。金属冶炼技术的出现与发展是金属货币广泛使用的物质前提。金属货币所具有的价值稳定、易于分割、便于储藏等优点，确非实物货币所能比拟。

第三个阶段：金属货币向信用货币形式转化。信用货币产生于金属货币流通时期。早期的商业票据、纸币、银行券都是信用货币。信用货币最初可以兑现为金属货币，逐渐过渡到部分兑现和不能兑现。信用货币在发展过程中，由于政府滥发导致多次通货膨胀，在破坏兑现性的同时也促进了信用货币制度的发展与完善。20世纪30年代，世界各国纷纷放弃金属货币制度，不兑现的信用货币制度开始登上货币历史舞台。

第四个阶段：货币的现在与未来——电子货币。电子货币作为现代经济高度发展和金融业技术创新的结果，是以电子和通信技术飞速发展为基础的，也是货币支付手段职能不断演化的表现，从而在某种意义上代表了货币发展的未来。随着移动互联网、云计算、区块链等技术的发展，在全球支付方式发生巨大变化的背景下，未来货币的形式将更加多元化和智能化。“数字货币”已不仅是一个概念，还正逐渐变成一种需求。尽管目前数字货币发行还面临科学技术、流通环境、法律规定等一系列问题，数字货币的魅力仍然难以阻挡。

伴随着货币形式的不断演化，世界货币体系也发生了相应的改变。这既是社会、经济、政治因素发展变化的结果，也是货币形式适应这一变化的转变。在19世纪初期，由英国主导的国际金本位制度运行了大约一个世纪。“二战”后，由美国主导的“布雷顿森林体系”确立，使美元成为唯一的国际储备货币，尽管在20世纪70年代，“布雷顿森林体系”崩溃，世界进入“牙买加体系”，走向多元化货币时代，但是美元仍旧占据主导地位。

全球经济一体化的发展和国际货币体系的演变产生了对创造超主权储备货币的需求，并使之成为一个古老且悬而未决的问题，那就是什么样的国际储备货币才能保持全球金融稳定并促进世界经济发展。历史上的银本位、金本位、金汇兑本位、“布雷顿森林体系”都是解决该问题的不同制度安排，也曾经有学者提出过建立国际货币单位“Bancor”的设想，也有当前建立SDR的实践。但是金融危机表明，这一问题不仅远未解决，由于现行国际货币体系的内在缺陷反而愈演愈烈。以比特币为代表的数字货币的出现，为超主权货币的出现提供了想象空间。那么数字货币是什么？

2. 数字货币

2014年欧洲银行管理局（European Banking Authority）给出了虚拟货币的定义，即“虚拟货币是价值的一种数字表达，它不是由中央银行或某个公共权威机构发行，也不一定与某一法定货币挂钩，但被自然人或法人接受用于支付手段，可以进行电子化转移、储藏或交易”。根据这一定义，虚拟货币包含三层含义：首先，虚拟货币是价值的数字化表示。虚拟货币具有一定的价值，且以数字化形式存在。它类似货币概念中的“记账单位”，也可以被看成是私人货币或商

品。其次，虚拟货币不是法定货币，因为它不是由中央银行或公共权威机构发行（任何由中央银行或公共权威机构发行的货币，不论其采用物理的或数字的形式，都属于法定货币）。目前金融体系中的电子货币属于法币而非虚拟货币。虚拟货币也不一定与法币挂钩，即它与法币没有固定的兑换比率。再次，虚拟货币可以具备“交换中介”的职能，被自然人或法人用作支付手段从他人处获得物品或服务；也可以用来进行电子化储存、转移和交易。不同的虚拟货币被接受和使用的范围不同，可以在很大的范围内被广泛接受，也可以只局限在某个社群内。

参照IMF研究报告的分类，我们可以把数字货币定义为“价值的一种数字表达”，它包括由非中央银行或公共权威机构发行的数字货币即虚拟货币，也包括中央银行或公共权威机构发行的数字化法定货币。下面将从数字货币的信用建立方式、发行方式、功能以及运行机制来看数字货币。

目前从数字货币的生成方式来看，主要有四种，分别是数字法币、基于算法的比特币、众筹发行和资产锚定。央行发行数字货币的前提是国家或者法律授权，尽管现阶段尚未出现，但法律授权将来也会成为数字货币发行的一种方式；比特币是一种算法货币；而众筹发行比较典型的代表是以太币，以太币如果希望基于区块链技术开发一个通用协议，也就是发布一个技术白皮书，并筹集资金来开发，那么就可以发行自己的以太币，以太币可以用来组织一个开发者社区，并实现在区块链上的应用；很多代币的产生，是可以把资产登记在区块链上的，以这个资产作为锚定物，来发行形形色色、各种各样的数字货币。

从建立信用的方式来看，一种是法币，一种是私人货币。数字货币如果是央行来发行的话是基于国家信用，而基于区块链上的通用私人货币，如比特币则是依靠算法来建立信用。以太币虽然也是算法货币，但是它和比特币的不同之处在于以太币的特定用途，当以太榜上智能合约的使用价值越来越高的时候，货币的价值也会随之上涨。

从功能上看，数字法币是履行传统货币的功能，即充当价值储存、价值标准和价值交换的手段。而以比特币为代表的算法货币最主要的是充当交换价值和支付工具的职能。比特币不合适成为价值储藏的手段是由于其币值波动太大。众筹货币主要是用来运行区块链各种各样的通用协议，比如要运行以太坊上的某种通用协议，就需要使用以太币来运行。而代币是锚定货币，锚定的对象是登记在区块链上的资产，是一种智能资产。

从数字货币的运行基础来看，数字法币是基于联盟链或者分布式总账系统技术来运行；比特币是基于公有链来运行；而众筹货币如以太币是基于区块链上的通用协议来运行；而资产锚定的货币——代币，主要是运行在区块链的商业应用上。

由此可见，数字货币以其不同以往的发行和运作方式，实现着传统货币的全部或者部分功能，并在某一领域使得货币的功能发挥得更加灵活和智能。相比纸币，数字货币优势明显，不仅能节省发行、流通带来的成本，还能提高交易或投资的效率，提升经济交易活动的便利性和

透明度，同时基于数字货币可以产生更多的应用，实现更为丰富的功能。此外，由央行发行数字货币还可能提升金融政策的连贯性和货币政策的完整性，数字货币超越时空的特性，也使得其在国际贸易和货币流通中发挥作用成为可能。

央行与数字货币——不可或缺的区块链

以比特币为开端，数字货币在2009年横扫世界。如果把数字货币的发展进程看成一场游戏，那么，比特币只不过是开启了游戏的按钮。中本聪可能根本没有想到，比特币竟然以投机炒作的方式进入了人们的视野。截至目前，中国是数字货币交易第一大国，全年交易量占到了全球交易总量的70%。随着数字货币市场的逐渐冷静，人们也开始以更加理性的态度来认识并实践数字货币，各国央行从不认可比特币到打算尝试数字货币无疑就是最好的证明。

1. 中央银行——现代货币体系的守望者

中央银行是国家最高的货币金融管理组织机构，在各国金融体系中居于主导地位。国家赋予其制定和执行货币政策，对国民经济进行宏观调控，对其他金融机构乃至金融业进行监督管理的权限。商品经济的迅速发展、经济危机的频繁发生、银行信用的普遍化和集中化，既为中央银行的产生奠定了经济基础，又为中央银行的产生提供了客观要求。

以美联储为例，美联储是美国联邦储备委员会的简称，其职能实际上就是“美国中央银行”。美联储成立于1913年，由全美12个地区的联邦储备银行组成。联邦公开市场委员会是它的货币政策决策机构，每年在华盛顿召开8次议息会议，决定货币政策的调整方向。它负责制定美国的货币政策，包括规定存款准备率、批准贴现率、对12家联邦银行和其他会员银行及持股公司进行管理与监督。其中，有四个基础政策工具：贴现率、公开市场操作、金融监管和调准备金率。

美联储在货币金融政策上有独立的决定权，直接向国会负责。一般来说美联储的货币发行是这样的：首先，美国政府通过预算案发行国债；其次，政府将发行的国债抵押给美联储；最后，美联储以收到的国债抵押数额发行货币——美元。

为了降低市场利率，刺激经济增长，2008~2013年，美国实施了四轮量化宽松政策，货币超发，美元泛滥，导致了美元的贬值与全球主要货币汇率的升值。汇率的剧烈波动加剧了全球贸易的不平衡，进而又进一步加大了全球经济的不平衡。2013年，美联储启动了量化宽松政策退出的按钮，并于2015年年底进入加息周期。美联储加息无疑将对包括中国在内的新兴经济体的资本流动和币值稳定构成压力。美联储加息就犹如一柄“达摩克利斯之剑”，悬于全球金融市场之上，所以世界各国都在时刻关注美联储的加息情况。

如今随着互联网、云计算、区块链等技术的发展，全球范围内支付方式也在发生着巨大的变化，数字货币的崛起对中央银行的货币发行和货币政策都带来了新的机遇和挑战。目前全世界发行了若干种数字货币，其中最著名的就是比特币。以欧洲为例，2015年，数字货币在该地区的交易额超过10亿欧元，总量虽然不大，但是来势汹汹。基于此，国际货币基金组织和各国金融监管机构，对数字货币及其依托的区块链技术开展了一系列的研究，并积累了一些重要的成果和实践经验。

比特币的崛起使得世界各地的央行行长们开始研究发行数字货币的可能性，到目前为止，还没有哪家中央银行愿意发行法定货币的数字化版本。比特币的出现，有便捷同时暗藏危险，有突破但是也带来了混乱。因此，世界各国央行对待比特币的态度又是怎样的呢？

2. 各国央行对待比特币的态度

对于比特币的监管，各个国家政策差异非常大。

（1）唱好方

美国。在美国加州率先让比特币合法后，美联储在虚拟货币上的野心也不小。早在2014年年底，美联储就发布了一份改善支付系统的白皮书，提出要研究一种加密货币。美联储在白皮书中提到，“和比特币一样，该加密货币将利用互联网的分布式架构的优势来降低直接通信的成本”。但不同于比特币，美联储的对象将是金融机构，而非个人用户，而且美联储所使用的术语是“point-to-point”（点对点），而非“peer-to-peer”（对等计算）。此外，比特币依赖于区块链技术，但美联储的项目所依赖的是一个中央总账系统和当局机关。

英国。英国央行堪称全球范围内对区块链技术兴趣最高的央行之一。在2016年1月的题为《分布式账本技术：超越区块链》的报告中，英国央行提到，正在探索类似区块链技术的分布式账本技术，并且分析区块链在传统金融业中应用的潜力。

不仅是金融领域，英国央行在上述报告中指出，去中心化账本技术在改变公共和私人服务领域都有着巨大的潜力。它重新定义了政府和公民之间的数据共享、透明度和信任。同时，英国央行已组建了区块链技术团队，英国央行行长卡尼在2015年9月也曾表示，考虑发行电子货币的可能性。

有分析认为，这主要源于英国央行正在寻求支付系统的创新支持，并希望能占区块链技术发展的先机重夺国际金融中心的地位。过去一两年，英国的银行自动清算业务系统发生了若干次故障，作为英国所有银行进行转账的主要方式，这一系统在2014年10月曾经一度中断服务9个小时。

德国。比特币在德国是一种价值单位。比特币行业在德国发展相对比较规范，已经纳入国

家的监管体系。政府表示，应把比特币当作私人货币和货币单位，个人使用比特币一年内免税，但是进行商业用途要征税。比特币由电脑网络发行，无须任何服务作为回报，因此被排除在电子货币的定义之外，尽管它履行了电子货币的相同经济职能，也有单独发行货币的实际能力。在德国，电子货币的法律概念只适用于那些最终源于真实货币的金融工具，因此比特币实际上被定义为一种商品。这类似于最近一些政府决定把比特币捐赠当作实物捐赠（如捐赠食品和物资）的做法。

2016年3月1日，德国联邦金融监管局公开了一份题为《分布式账本：虚拟货币背后的技术区块链为例》的内部报告，对分布式分类账本在跨境支付中的使用，银行之间转账和交易数据的储存等领域的潜在应用进行了探讨。德国联邦金融监管局是德国金融监管的主体，成立于2002年，有权监管包括银行、金融服务机构、保险公司在内的所有金融机构，并且可以依法对被监管对象进行处罚。不过，它看起来具有为金融市场建立一个新标准的潜力。不过，德国联邦金融监管局也提醒，需要注意区块链技术在应用中可能会出现风险，并继续呼吁世界其他的监管机构对区块链进行更加严厉的监管。

（2）唱衰方

泰国。全面封杀比特币。2013年7月30日，泰国外汇管理和政策部的高官表示，由于缺乏适用的法律和资本管制措施，加之比特币跨越多种金融业务，因此下述比特币活动在泰国都被视为非法：买卖比特币、用比特币买卖任何商品或服务、与泰国境外的任何人存在比特币的往来。泰国比特币创业公司Bitcoin Co表示，由于泰国央行封杀了比特币，因此该公司将停止所有业务。泰国成为在世界各国中封杀比特币的首例。

未来，随着各国监管部门对数字货币的了解加深，各国政府对数字货币的监管政策会越来越明晰，央行发行数字货币也逐渐成为可能。

3. 中国对待比特币的态度从否定、质疑到肯定

IMF认为数字货币技术具有改变金融的潜力，而且在清算和结算方面具有独特的优势。中国人民银行从2014年开始就成立了专门的研究团队，对数字货币的发行和业务运营的框架、关键技术，对经济、金融体系的影响，以及相应的监管方面的挑战，进行了深入的研究。

中国目前是数字货币交易量第一大国，2015年比特币的全年交易量占全球交易总量的70%。中国数字货币交易所的产品、安全性及用户体验也远远超过国外的交易所。比特币在中国的发展经历了“接受—认可—爆炒—下跌”的阶段，到现在，人们对比特币的认识更加趋于理性化。

在2013年12月5日的央行等五部委公布《关于防范比特币风险的通知》之前，比特币交易市场发展得如火如荼，比特币成为各类媒体争相报道的热点和焦点，并在一定程度上引导了更多

的热钱涌入投机市场，大量民众参与其中，直接推动比特币在2013年11月24日上涨至1242美元的历史最高位。交易平台普遍存在以“网络货币”“未来趋势”“数字黄金”等煽动性炒作误导民众的问题；另外“融资融券”和“杠杆交易”等高风险交易也增强了虚拟商品的投机性。此现象引起了央行的关注，2013年12月5日，央行等五部委立即发布《关于防范比特币风险的通知》，抑制比特币的过度投机。该通知明确了比特币不是央行发行的货币，不受法律保护，同时要求各金融机构和支付机构不得开展与比特币相关的业务，明确加强对互联网网站的管理，进行网站备案等工作，防范比特币洗钱风险等事项。

通知一公布，比特币就开始进入震荡下跌的进程。尽管如此，仍有不少交易所选择在此时进入市场，理由是“法不禁则可为”。2014年3月，央行再次向各分支机构下发了一份名为《关于进一步加强比特币风险防范工作的通知》，要求各银行和第三方支付机构在4月15日前关闭境内所有比特币平台的所有交易账户。此举意味着金融机构为比特币网站平台的交易账户开户为不合法，投资者无法在中国境内为交易进行银行转账和第三方支付。

2014年4月11日，央行行长周小川在博鳌亚洲论坛上发表言论，“比特币本来不是央行启动的，也不是央行批准的一个币，我们谈不上什么取缔。与集邮者收集的邮票一样，邮票上虽写有价钱，但主要是收藏品，人们把它当作资产来进行交易。比特币也一样，它更像是一种能够交易的资产而非支付货币，所以，对于央行来说不存在是否取缔的问题”。随后，央行编写的《2013年中国人民银行规章和重要规范性文件解读》一书出版，书中提到央行发布《防范比特币风险的通知》主要是为了防范虚拟商品的投机风险、洗钱风险及其他风险。

2014年底，央行原副行长吴晓灵在财经国际论坛上谈及算法货币，她把类似比特币的数字货币定义为算法货币。其核心内容主要在三个方面：

一是算法货币只解决了信用问题，但如果没有适应经济需求的供给调节机制，就无法解决币值波动问题。它可以成为金融产品、金融资产，但无法成为一个好的货币。

二是算法货币能否成为货币取决于参与者的认可和币值的稳定。法定数字货币的支付结算与法定货币可兑换的算法货币的支付结算，必须满足监管的要求，做到交易过程可溯源。以目前的分布式跨境支付的研发状况，它还只能是现有国际清算体系未来的挑战者，现阶段会是多种支付协议的研发和并存。用信息技术构建价值传导网络是值得探讨的方向。

三是法定货币之外的货币为私人货币，私人货币有实物形态，也有数字形态，数字形态的私人货币可以与法定的电子货币共存。

2016年1月20日下午，中国人民银行召开数字货币研讨会，探讨了数字货币和区块链等技术，并很快在央行官网上发布会议公告。从公告全文来看，中国央行对于区块链等数字货币技术高度肯定，表示将会积极研究探索央行发行数字货币的可能性，并且首次表示发行数字货币

是中国央行的战略目标。这一态度无疑对数字货币和区块链技术在中国的发展有极大的促进作用。

央行探索发行的数字货币，首先，是一种法定货币，具有法定货币的一切职能，与流通中的现钞具有一样的价值。其次，这种数字货币有可能采用某些加密货币的优势技术（如区块链技术）和交易模式（如点对点直接交易），提高金融交易透明度，有效防范洗钱等犯罪行为；还可以提高金融交易效率 and 安全性，使金融交易的清算时间、交易成本和交易对手风险得以降低；同时，这一数字货币体系不大可能采用完全去中心化的数字加密货币模式，而很可能采用一种完全创新的混合技术架构。

总体来说，央行对数字货币的态度从质疑、否定到逐步认可，这一转变实际上是关注对象从比特币到区块链技术以及未来形式更为丰富的数字货币的转移。随着央行对于数字货币的研究和解读越来越清晰，数字货币的发行越来越成为可能。数字货币和现有货币体系的融合无疑将加速数字货币在全球范围的发展。

Fintech（金融科技）创新最前沿——区块链技术

在这个变化日新月异的时代，唯有“创新”是不变的真理。如何利用技术更好地发展行业，为消费者带去更便捷、更方便、更优质的体验，是各行各业中每个人都不可忽视的问题。随着互联网对日常生活渗透率的不断加深，人们行为的数字化成为现实。由于金融行业对于信息和数据的高度依赖，数据分析技术对于金融行业的改造既具备了必要的技术基础，又有其现实需求，投资界甚至为这类创新创造了一个新词“Fintech”，从这个单词的构词方式上也不难看出其与金融和技术创新的关系。那么Fintech将给金融行业以及我们的未来带来何种变革呢？

1. Fintech——科技创新变革金融

随着互联网在人们生活中的普及度越来越高，人们越来越离不开手机、离不开网络，出现了各种打车软件、外卖软件、手机支付、理财app，似乎生活中的一切包括金融理财都能通过互联网来完成，给我们带来了更便捷、更低成本的使用体验。Fintech更贴切地描述了互联网公司或者高科技公司利用云计算、大数据、移动互联以及区块链等新兴技术开展低门槛的金融服务。沃顿商学院给出的Fintech的释义是：用技术改进金融体系效率的经济行业。

如今，全球各大金融机构运用云计算、大数据、移动互联等技术概念，优化便捷客户的使用体验。比如银行建立生态圈，让客户在旗舰店、全功能网点、简易型网点、ATM和电子银行间自由选择，无缝衔接各服务流程；利用大数据统计客户的偏好习惯，根据不同客户不同的生命周期，在不同阶段提供灵活组合的贸易融资产品、工具和资产配置服务方案；利用硬件软件

技术创新，为客户在跨境贸易方面提供最优资金汇划路线和最佳收费模式，等等。这些科技创新可谓实实在在地改变了我们的生活方式、投资理财方式。如今，美国排名前100的金融科技公司的业务范围包括借贷、支付、数字化货币、交易、投资和资产管理等全部传统金融机构的业务领域，其他覆盖领域包括保险、众筹、外汇、零售银行和征信等。成功的金融科技公司的商业模式可归纳为四条策略：通过与B端合作的模式批量获取有效C端客户；利用互联网和移动设备为客户提供纯线上服务，简化业务流程、优化产品界面、改善用户体验；运用大数据和云计算提供基础信息支持，实现金融服务个性化；以细分市场作为切入点，专注服务特定类型客户，并提供相关增值服务。

金融科技公司致力于利用科技为客户提供更好的金融服务，包括提高金融服务的效率和降低金融服务的成本。信息技术的运用增加了金融服务的受众数量并提高了金融服务的频率，因而扩大了整个金融服务市场的规模。虽然，传统金融机构受到了来自新型金融科技公司的冲击，但是金融科技带来的最大影响是满足了过去传统金融机构无法实现的金融需求，服务了过去未被服务的客户，其实质是降低了金融服务的门槛，使普惠金融成为可能。从数据方面来看，2015年中国的金融科技服务金额高达27亿美元，印度也超过了15亿美元，美国的此类风险企业更是吸引了大约74亿美元的投资。通过这些数据，我们不难感受到Fintech如今在全球的火热程度。

支付可以说是最先让普通大众感受到科技改变生活的行业之一。支付业务的核心在于高效和低成本。以往我们习惯于银联刷卡、现金支付，如今拿着一部智能手机就基本能够行遍天下。支付公司和连锁商户进行合作，除了能快速获得客户量，更是让客户在生活的方方面面感受支付的变革。大部分支付公司致力于为商户提供界面清晰、流程简便的收款服务，支持线上、移动和线下多种场景的支付，如瑞典的Klarna和美国的Stripe，以及中国的支付宝和微信支付等。

网络借贷近年来吸引了大量投资者，也可以说是普通大众最熟悉的金融科技领域之一。互联网平台帮助金融实现脱媒，帮助以往难以获得银行贷款的中小企业和个人消费者满足融资需求。2014年12月，美国的Lending Club成为第一家上市的P2P借贷公司；2015年12月，宜人贷赴美上市。虽然说我国近来也有P2P平台涉嫌非法经营，跑路事件频发，但从整体上看网络借贷行业还是在稳步前进的。网络借贷的优势在于借款方式灵活简便、利用互联网等大数据征信技术对借款人进行筛选，能够针对未被银行覆盖的信贷潜在用户群体。互联网借贷能够与消费金融、供应链金融等结合，产品覆盖车贷、房贷及各类消费贷款。对于网络借贷公司而言，征信技术是核心能力，能够利用互联网技术收集更为广泛的信息，通过大数据分析和机器学习算法为借款人进行信用评级以及为投资者进行风险评级，能够为借贷两端都提供个性化的信用服务。目前网络借贷公司主要切入细分市场，总体来说，网络借贷的客户主要为中小微企业和个人消费者，但每家公司的业务切入点各有不同。有专门针对零售服务行业小企业的借贷公司，如另一家美国的上市公司OnDeck；有专门为潜在成功人士提供助学贷款和消费贷款的P2P借贷

平台SoFi，在提供贷款的同时，平台还提供职场辅导和创业辅导，并组织各类社交活动，助力借款人的事业发展；另有为学生和年轻白领提供分期付款的公司，如美国的Affirm和中国的趣分期等。

信用是金融行业的核心，征信技术也可以说是Fintech的核心，利用科学技术来解决金融脱媒，那么对客户进行各个维度的数据收集并进行信用评级就显得尤为重要。比如美国老牌数据公司FICO，其利用FICO模型得出的FICO分在美国绝大多数金融机构都得到了认可。在Fintech时代，FICO通过电信运营商数据、水电煤数据、金融交易数据等判断个人的征信状况；而在我国也有很多大数据征信科技公司，比如量化派、神州融等，通过与各大电商、银行、社交平台、门户网站及征信机构进行数据对接，构建自有模型来对借款人进行风控打分，从而把控网络借贷等行业的风险点。

但如今的金融科技公司还处于Fintech1.0阶段，技术创新仍在继续，而且可以说科技是Fintech的核心竞争力，未来更大的技术创新空间属于区块链技术。区块链，或者说是分布式总账技术的安全、透明、快捷、去中心化、低成本的技术特性对当前的金融系统来说是完美的补充，从加密货币，到智能合约，再到超越货币、经济和市场的公正应用，区块链技术有潜力变革的产业可谓非常多。目前，Fintech依托的技术还大多基于互联网为全球带来的沟通互联与数据便捷，而区块链将彻底变革我们目前所拥有的技术。区块链给全球带来的变化很可能就像当年互联网为世界带来的变化一样，会颠覆很多传统的产业，改变生产生活线。

2. 从“币”到“链”，区块链能带来什么

谈到区块链，我们就会想到比特币。从技术角度来看，比特币有三层：区块链、协议以及货币。第一层是底层技术，也就是区块链是去中心化的、公开透明的交易记录总账，其数据库是由所有网络的节点共享的，由矿工更新、全民监督，但没有人真正拥有和控制这个数据库；第二层是协议，即区块链上进行资金转账的软件系统；第三层是货币本身，如比特币。不只是比特币，可以说这三层的技术结构对所有的加密货币都是通用的，每一种不同的数字货币对应它独有的货币、协议以及区块链。

在区块链技术出现之前，数字货币和数字资产都有着无限可复制的特点，可信赖的第三方机构如银行、支付宝等履行着中心化媒介的角色，帮助双方确认一笔资产是否被花掉。而区块链点对点的分享技术以及公钥、私钥加密技术将货币的拥有权改为公共总账来记录，且不需要中心化机构，彻底实现了“去中心化”这一特点。

目前数字化货币还存在着一些问题，比如说从目前来看一旦私钥丢失就无法找回数字货币，而普通用户普遍没有很好保存私钥的能力，这也是比特币目前没有广泛流行的原因，但Circle等公司正在试图为客户提供备份保存的解决方案。基于区块链的现实应用，美国出现了Bitpay和Coinbase等这些成熟的比特币支付方案提供商。但目前商户面临传统支付、比特币支付

两套系统独立运行的问题，影响用户体验。Intuit通过PayByCoin模块在传统支付上集成了Bitpay和Coinbase支付，国内方面如果支付宝、微信能切入，将极大地促进数字货币的普及率。目前比特币的交易还是在用法币结算，其价格波动性也是数字货币未被广泛使用的因素之一。由此也出现了和美元锚定的Ripple；Bitpay和Coinbase也提供了法币、比特币实时转换的解决方案。区块链技术在国际汇款方面也有着极大的潜力，时效性、低成本都是区块链技术能够带来的优势，目前传统国际汇款交易费率为7%~30%。

比特币可以说是以更宏观的视觉来看市场，利用区块链技术对整个市场去中心化，通过区块链技术转换不同的资产来创建不同资产单元的价值。金融的本质是信任，交易双方或多方通过建立合约来履行信用，而去中心化的区块链技术帮助交易多方共同维护信用。区块链技术的去中心化账本功能可以被用来注册、确认、转移各种不同类型的资产及合约。所有的金融交易都可以被改造成在区块链上使用，包括股票、私募股权、众筹、债券、对冲基金和所有类型的金融衍生品，如期货、期权等。

区块链可以用于任何资产的注册、存储和交易，包括有形资产和无形资产。智能资产能够通过区块链控制所有权，并通过合约来符合现有法律。说到智能资产，就不得不提到智能合约。智能合约的出现意味着区块链交易远不止买卖货币，智能合约就是以数字编码的形式定义承诺。交易双方无须彼此信任，因为交易都是由代码强制执行的。比如，基于区块链的众筹平台主要是以支持初创企业创建数字货币来筹集资金，分发“数字股权”给投资者，这些数字货币作为支持初创公司应获股权的凭证。可以说，区块链能够极大地降低初创公司股权确权的成本，也保证了早期投资人在未来的合理收益。在审计等金融服务机构中，区块链超高透明度、实时又不可篡改的特性能够大大节约审计人员的审计时间及人力物力成本，降低第三方服务机构作假的概率。如要通过智能合约和智能资产来记录和转移更多复杂的资产类型，那么这也就需要强大的脚本系统即最终实现图灵完备（能够运行任何货币、协议和区块链）的系统提供支持，以太坊就是一个以区块链为基础的项目，旨在提供一个具有图灵完备属性的技术平台。

在金融领域以外，区块链技术的价值转移和信用转移特性也有很大潜力，例如在数字身份验证、公证和知识产权保护、音乐及医疗等领域。

3. 各大金融机构纷纷抛出橄榄枝

华尔街是美国纽约市曼哈顿区南部从百老汇路延伸到东河的一条大街的名字，是英文“Wall Street”的音译。“华尔街”一词如今已超越这条街道本身，更指对美国经济乃至全球经济具有影响力的金融市场和金融机构。华尔街金融机构的走势动向一直为全球金融从业人员所关注，而华尔街也不乏很多金融行业的明星人物。摩根大通前高管，人称“华尔街女皇”的Blythe Masters（布里特·马斯特斯）就是其中的一员。

“华尔街女皇”在摩根大通工作过27年，对摩根大通金融衍生品业务做出过杰出的贡献。她

是华尔街曾经的大宗商品交易界的“一姐”，28岁成为董事总经理，创下摩根大通史上最年轻的女高管记录，她担任过摩根大通多个高管职位，包括首席财务官。作为CDS（信用违约掉期，Credit Default Swap）之母，她构思的金融衍生产品市场规模一度高达58万亿美元，也被认为助推了2008年的金融危机。2014年Blythe Masters在摩根大通辞职，沉寂一年之后，出任数字资产控股（DAH，Digital Asset Holdings）的首席执行官，再度引起全球关注。DAH公司的产品主要是为金融机构的结算与清算提供分布式账本解决方案。Blythe Masters在华尔街大力倡导和宣传区块链的解决方案，因此也被华尔街同行以及媒体称为“区块链女皇”。

2016年2月，DAH宣布，投行界巨无霸高盛和蓝色巨人IBM也加入了其最近的一轮融资，这使得DAH在A轮融资的总金额上升到了6000万美元，这是迄今为止私有或者授权区块链创业公司获得的最大一笔投资。而投资方的来头也都非常引人注目，现在它已经获得了14家金融机构的支持，除了高盛和IBM，本轮融资的其他参与方还包括荷兰银行、埃森哲、澳洲证券交易所、法国巴黎银行、Broadridge金融解决方案、花旗银行、CME Ventures、德意志交易所集团、ICAP、桑坦德风投、证券托管清算公司（DTCC）以及PNC金融服务集团。本轮融资也标志着高盛开始参与比特币和区块链领域的第二笔公开投资，上一笔是发生在2015年，高盛领投了比特币服务提供商Circle的5000万美元融资。高盛全球联席技术主管保罗·沃克在一次声明中表示，高盛非常相信分布式账本技术对于金融机构在全球范围内交易所将扮演角色的重要性，这将是变革性的，高盛将非常期待与DAH以及其他金融机构和技术社区一起参与到区块链的技术发展中来。DAH瞄准的市场包括银团贷款、美国财政部回购、外汇、证券结算以及衍生工具等。在其A轮融资之中，他们获得了澳洲证券交易所的千万美元合同，为澳洲证券交易所设计利用区块链技术的证券交易结算系统。澳洲交易所可以说是分布式账本生态系统中的领航者之一，非常有可能成为全球最早应用区块链技术的证券交易所。其非常看重区块链技术所能节约的证券结算成本、股权确权成本以及高透明度等特点。

除证券交易方面外，澳大利亚银行业热衷于区块链在节约成本与安全性上的潜力。目前澳大利亚所有主要银行都加入了全球金融创新公司R3CEV（以下简称R3）运行的区块链项目。

R3是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟在2015年末最初一轮的合作中已经吸引了42家巨头银行，其中包括桑坦德银行、摩根大通、富国银行、美国银行、纽约梅隆银行、花旗银行、德国商业银行、德意志银行、汇丰银行、三菱UFJ金融集团、摩根士丹利、澳大利亚国民银行、加拿大皇家银行、瑞典北欧斯安银行（SER）、法国兴业银行，等等，可以说是全球范围内最大的银行“拥抱”区块链联盟。2016年3月，R3宣布开始接受新的合作伙伴，而近期日本SBI控股成为首个在第二轮宣布加入该联盟的金融机构，从总数上来看，R3联盟已经与43家全球巨头银行达成协议。与R3合作的技术供应商目前有5家，分别是Eris Industries、以太坊、IBM、英特尔与Chain公司，R3还使用了微软Azure的区块链即服务

（BaaS）。目前由R3引导的金融机构联盟已经与40家银行合作完成了5个不同的区块链解决方案，主要针对商业票据、大型企业所使用的短期债权证券等，参与的客户银行可模型化金融资

产、商业票据、短期债务工具，可以进行创建、购买或出售以及赎回操作。R3负责人表示目前各项模拟测试都会选择较少数量的合作银行分成小群体来进行试验，目前模拟测试已经进行了至少600笔交易，不过测试交易中都没有使用到真正的资金。在每次测试结束后，技术供应商都会向参与的银行展示他们的工作，让R3客户直观地了解底层技术。而在每次测试后，所有R3联盟银行包括没有参与试验的银行都能够共享研究成果。这也是如此多顶级金融机构都趋之若鹜地加入R3联盟的因素之一，任何金融机构都不想在新技术的成长期掉队，掌握技术就是掌握未来。

全球各大顶级金融机构的高管也都纷纷发言表示对区块链技术的看好。巴克莱投资银行的首席技术官Brad Novak表示，巴克莱已经在共享式账本以及智能合约的价值评估上取得进展，期待能够利用R3实验室来协同技术实验，并期待合作实验室能够利用各种知名开源技术。汇丰银行全球银行和市场部首席信息官理查德·赫伯特表示，R3全球访问实验环境以及R3联盟能够帮助R3联盟中的会员银行合作共享实验成果及智能合约等技术。瑞银高级创新经理Alex Batlin则表示，将参与实验的银行连接到一个模拟现实世界的网络中，将理论进行试验，验证如何有效地在安全环境中运行是非常重要的。桑坦德银行则表示，R3为他们提供了一个与其他金融技术平台协同合作建立一个基于加密货币和分布式总账技术新平台的机会，并表示桑坦德银行热衷于推动这一合作，为塑造日后金融行业发展的新平台而努力。荷兰银行和金融服务集团ING也是R3区块链联盟成员之一。ING的全球交易服务主管Mark Buitenhok（马克·布特何克）接受Coin Desk采访时说，ING正在积极推进探索区块链技术的进程，这个探索过程是具有深远意义的，与世界各地知名银行共同参与联盟合作探索区块链技术并能在内部进行跨行、跨部门的区块链技术更是能够带来实践意义。Mark Buitenhok表示，ING认为区块链在银行和金融环境中有很多应用的潜力，包括证券和交易结算、内部办理、电子身份，也可以作为连接不同设备的支撑网络。

超级账本Hyperledger是Linux基金会于2015年发起的推进区块链技术和交易验证的开源项目，目前它已得到了30家大型公司的支持，包括思科、摩根大通、英特尔、富国银行、伦敦证券交易所、IBM、区块链公司DAH、R3、荷兰银行、埃森哲、芝加哥交易所集团等，成员分布之广也体现了金融与技术的多样性。正如Hyperledger官方网站上的描述，这一项目的目标是发展一个跨行业的开放式标准以及开源代码开发库，允许企业创建自定义的分布式账本解决方案，以促进区块链技术在商业当中的应用。全球各大顶级金融机构给予的支持也体现了金融、技术机构对此开源项目的认可。自从2015年12月计划成立该项目，超级账本项目已经收到来自多个企业的代码和技术，其中包括Blockstream、DAH、IBM和Ripple等，其他社区成员也在考虑如何贡献他们自己的力量。Hyperledger项目是让成员共同合作，专注于开放的平台，以在将来满足多个不同行业各种用户的案例，简化业务流程。

“成百上千的金融科技创业公司正在硅谷崛起，它们拥有大量的智慧头脑和风投资本，而他们正在做的事情就是开发出针对传统银行业的替代技术。”这是摩根大通董事长兼首席执行官杰

米·戴蒙在致股东的信中所说的。摩根大通也参与了R3区块链联盟、Linux基金会牵头的超级账本Hyperledger账目以及摩根大通前高管领导的DAH区块链公司。据摩根大通的首席营运官马特·赞姆斯说，摩根大通计划在2016年增加对整体技术的资金投入，从2015年的92亿美元增加到94亿美元，其中40%的预算用于新投资和新技术，这将包括与新兴公司的合作。由此不难看出，摩根大通对于金融科技的重视程度。摩根大通大幅度增加对于技术创新的资金投入，积极参与各大区块链联盟项目，就是希望能够掌握最前沿的区块链技术，通过区块链技术来帮助货币结算，为客户提供更快的周转时间、降低银行风险。据《华尔街日报》报道，摩根大通已经悄悄地在测试区块链技术用于美元汇款的可行性，测试汇款在伦敦和东京两个金融中心之间进行，大约有2200名客户参与。在其新的区块链计划中，据摩根大通的企业及投资银行的首席行政官萨诺克·维斯瓦纳坦透露，摩根大通计划尽快扩大其对真实交易的测试，第三季度会为某些企业和投资银行的客户，包括一些对冲基金，开展区块链测试等。

区块链技术的实时、不可篡改、高透明度等特性完全匹配审计行业，能够提高审计透明度及各类成本、因此四大会计师事务所都在马不停蹄地探索区块链技术。经过大约一年的研发时间，德勤率先推出了区块链一站式平台Rubix。这一基于区块链技术的平台不仅能够提高审核购销的速度以及透明度来节约审计成本、降低造假成本，还有望帮助企业客户完成咨询工作。

德勤的竞争对手，审计巨头普华永道也推出了类似计划，试图使用区块链来服务市场。2016年1月，普华永道宣布与Blockstream公司达成战略合作伙伴关系，根据Blockstream官网的新闻稿表示，这一合作旨在为世界各地的公司提供区块链技术与服务。随后普华永道也成立了一个区块链顾问团队，英国主要金融监管机构的一名前监管者，已被普华永道公司聘请加入这个最新成立的区块链顾问团队。2016年2月，普华永道又与DAH达成战略合作伙伴关系，DAH将为其提供区块链技术支持，帮助其节约时间和成本。随后普华永道公布了基于区块链技术的解决方案组合，旨在帮助其商业客户从区块链解决方案的构想阶段一步步接近实际应用。普华永道的区块链解决方案组合由12项服务组成，涵盖了目前主要金融机构热议的应用分析，功能主要集中在教育、评估，通过这一套解决方案组合，普华永道希望加强其与客户和行业合作伙伴之间的协作。普华永道Fintech高管杰里米·德雷恩对普华永道的新服务感到非常自信，他解释这是为了帮助公司了解区块链给金融服务带来影响的规模和范围。

在金融科技、区块链如此火热的表面下，我们也要理性地看待技术创新而不是一股脑地去热炒。区块链确实重要，全球顶级金融机构的高管都难以否认这样的事实，但是根据普华永道最近的一份高管调查显示，有些金融机构对采用区块链技术，仍然保持了谨慎的态度。

从概念上来讲，区块链和银行业应该是完美的合作伙伴：一个分中心化的数据库可允许股票或债券交易近乎实时地进行交易，将交易记录在一个难篡改、难摧毁的链数据库上，无须中间商或清算所的参与，更将繁重的处理成本、长时间的结算时间和人为错误风险都从理论上根除。而以往为防止违约风险的宝贵资本和抵押品也变得可有可无。据区块链创业公司SETL估

算，每年清算和结算交易的成本高达800亿美元，如果能够削减其中的一定比例，那对于银行业来说可谓是降低了很大的成本费用，但将理论彻底实践起来还是存在着一些目前看来不可逾越的差距。比如如何让清算所、交易所和经纪公司同意一种新的系统，而它是否会对其现有的盈利造成冲击？监管问题又如何解决？况且银行自身就聘请了大量的中间商，无论是抵押贷款经纪人还是销售商，这些中间商在这样一个直接交易的世界里又如何能够生存下去？以上所有的这些问题，使得区块链对银行的吸引力显得并不是那么强烈。难怪瑞银在2016年1月的白皮书中，将这种技术描述为一把“双刃剑”。当然，金融科技的创新，尤其是区块链技术的出现显然是未来的大势所向，只不过还需要时间和资金的投入，但是对于金融机构来说如果不走在技术创新的前列，难免不会被未来的浪潮拍在沙滩上。

金融拥抱区块链

支付汇款——变革的前夜

比特币于2009年诞生之始，也许只是微露曙光，理想主义者便敏锐地嗅觉到了“世外桃源”的味道。于是乎，比特币以摧枯拉朽之势，被挖掘、被追逐、被高高捧起，成就了一批新富的狂欢，接踵而至的是一些人的伤心和迷惘。“挖矿”已经蜕变成一场比较算力的游戏，挖出比特币的同时，也挖出了人性的贪婪。当比特币堆积的泡沫不断膨胀时，心灰意冷的不仅是设计者（它的发展已经与设计者的初衷相背离），也使得理想主义者心生悲凉。然而，待繁华褪尽，赌徒似的交易者离场之后，经过人们的努力，比特币终于走出了自由主义的小圈子。人们开始思索比特币最终给世界带来的是什么。回到理想主义的源头，我们看到了比特币所信奉的自由、平等的价值理念，也开始关注比特币背后的区块链技术。

支付汇款已经成为人们日常生活的重要组成部分。而区块链技术的运用让支付变得更为快捷、便利和实惠。区块链技术的介入，能够让虚拟货币像流水一般在网络上流淌，没有延时，没有折损。区块链技术将催生出一个全新的支付汇款方式，挑战着庞大而臃肿的传统机构。比如Ripple（瑞波）协议创造了一个比特币投资价值网络支持的去中心化的支付体系，试图让不同货币自由、免费、零延时地汇兑，挑战着SWIFT（环球银行金融电讯协会）的生存空间。技术的突破、资本的加码、政策的默许，也许这是一个变革的前夜。原来，比特币才是前奏，一席大幕正徐徐拉开。

1. 不简单的支付

汇款是人们日常生活的基础内容之一，微信逐渐普及之后，微信红包不仅将汇款的社交功能明显强化，甚至赋予其娱乐的功能，毕竟在强大的数据处理能力的支持下，人们之间的转账太方便了，这种便利实际上是几百年来金融业务和现代科技共同发展的结果。15世纪之初，正是威尼斯商人对大量的汇兑业务的处理才促成了现代银行的诞生，进而又衍生出商业银行“存、贷、汇”的基本职能。事实上，银行汇款已经发展成为银行接受客户的委托，利用一定的工具，通过资金头寸在代理行或者联行之间的划拨，将款项交付给国外收款人或债权人的结算业务。汇兑两地属于两国时，即为国际汇款。一般来说汇款的种类有三种，即信汇、电汇和票汇。如下图3-1所示。

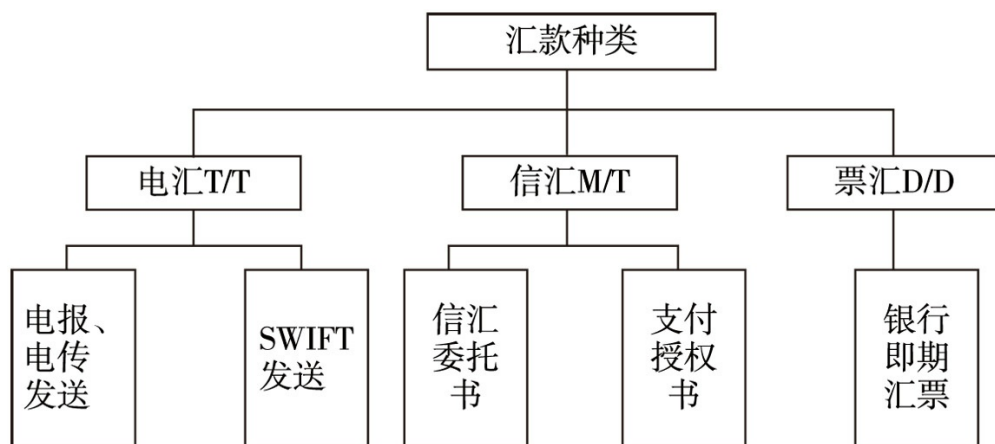


图3-1 汇款的种类

资料来源：2015年3月普华永道对544位金融高管的调查

(1) 汇款的种类

信汇（Mail Transfer，简称M/T）。进口人（即债务人或称汇款人）将汇款及手续费交付给汇款地的一家银行（汇出行），委托该银行利用信件转托收款人所在地的银行（汇入行），将货款付给出口人（即债权人或称收款人）。这种汇付方法，需要一个地区间的邮程的时间，一般航邮约为7~15天，视地区远近而异。如用快递可以加速3~5天。

电汇（Telegraphic Transfer，简称T/T）。汇款人将一定金额的汇款及汇付手续费付给当地一家银行（汇出行），要求该银行用电传或电报通知其国外收款人所在地的分支行或代理行（汇入行）将汇款付给收款人。这种汇款将时差计入，一般当天或隔天可到，最为快捷，但电汇费用比较高。

票汇（Demand Draft，简称D/D）。汇款人向其当地银行（汇出行）购买银行即期汇票，并直接寄给收款人，收款人收到该汇票即可去指定的付款银行取款。这种银行汇票和逆汇法的商业汇票不同，银行汇票用于银行的代客拨款，故受票人和付款人是同一银行（或代理行）。

电汇是以电报或电传作为结算工具；信汇是以信汇委托书或支付委托书作为结算工具；票汇是以银行即期汇票作为结算工具。票汇与电汇、信汇的不同在于票汇的汇入行无须通知收款人取款，而由收款人持票登门取款。汇票除有限制转让和流通者外，经收款人背书，可以转让流通，而电汇、信汇委托书则不能转让流通。

如今，越来越多的市民愿意选择银行卡汇款，只要提供对方姓名和卡号，即可实现异地无卡存款，多家银行都已开通此业务。汇款地分布是否广泛，汇款支取是否方便成为考虑的重要指标。而眼下，随着电子汇款渠道的普及以及第三方支付的发展，更多的人启用网银、手机银行汇款。尤其是在国际汇款时，更倾向于选择电子汇款以及网络汇款的方式。

（2）国际汇款的五种渠道

电汇最常用、最主流，但花费高。据了解，目前市民办理境外汇款业务大多是通过电汇办理，这分为外汇汇款和外钞汇款。在办理电汇业务时，需要向银行准确提供汇款货币及金额、收款人姓名及地址、收款人开户银行账号、收款人开户银行名称、SWIFT码及地址或者中转行的SWIFT代码。

银行电汇要支付三项费用：一是汇款手续费，二是汇款过程中的电讯费，另外不可忽视的是“钞转汇”的费用，也就是说使用人民币现钞或者美元等外币现钞办理汇款业务，都会被要求按当日的汇率缴纳钞汇差价费用（汇款本金×当天的现汇卖出价/当天的现汇买入价-汇款本金）。此外，在汇款过程中，中间机构会收取一定的费用，要保证收款人收到既定的金额，一般还需要多汇一些，并在人民币账户中多锁定一些备用金，以防预期外的手续费产生。由于时差原因和是否需要中转等原因，汇出的款项通常在3~5个工作日到账，最快第二天到账。各家银行的手续费最低和最高限额有所不同，如表3-1所示。

表3-1 部分银行办理国际电汇业务的收费情况说明

银行	手续费费率 (按汇率金额计,‰)	手续费最低 限额 (元)	手续费最高 限额 (元)	电报费 (元)	电汇时间 (工作日)
工商银行	1	20	200	100	2~3
建设银行	1	20	300	80	3~5
中国银行	1	50	260	150	2~3
农业银行	1	20	200	80	3~5
交通银行	1	50	200	150	3~5
招商银行	1	50	200	150	5
民生银行	1	50	200	125	3~5
兴业银行	1	50	200	150	5
中信银行	1	20	250	100	3~4
邮政银行	0.8	20	200	70	1~2

以中国银行为例，汇款手续费按照汇出汇款金额的1‰，最低50元/笔，最高260元/笔收取；电讯费标准为港澳台地区发电80元/笔，国际发电150元/笔。

网银国际汇款。以往，涉及外汇外币的很多业务需要亲自到银行柜面办理；现在，通过网银就可以在家操作完成。目前很多银行都已经开通网银境外汇款业务。

在国内网银办理境外汇款，一般汇出者的储蓄卡须是用大陆居民身份证开立的，且外汇额

度够用，而收款人账户需为个人账户、学校账户或慈善机构账户，暂时不支持对境外公司账户转账。而填写申请时的信息和到账时间则与在柜台办理无异。

值得一提的是，用网银办理境外汇款的话，相比柜台办理可以获得一定的手续费优惠。

支付宝。日前，上海银行国际汇款业务正式进驻支付宝钱包，通过其“国际汇款”服务窗和应用，支付宝实名用户可以手机办理跨境汇款。

与传统的银行电汇不同，支付宝钱包的“国际汇款”服务支持24小时手机办理跨境汇款。用户只要下载并登录最新版支付宝钱包，在首页选择“国际汇款”应用或者关注“国际汇款”服务窗，即可使用由上海银行提供的国际汇款服务。汇款时，用户只要填好收款人姓名、国家、银行账号、币种、金额等必要信息，并用人民币完成支付后，就可以实现境外汇款办理，上海银行会快速完成后续货币兑换汇款操作。通常情况下，3~5个工作日就可以到账。

目前，支付宝钱包的“国际汇款”服务窗支持美元、欧元、港元、加拿大元、澳大利亚元、瑞士法郎、英镑、新加坡元、日元九大币种的汇款。

visa汇款的优势是手续简单。visa汇款服务也是一种比较方便实惠的境外汇款方式，并支持7×24小时办理。与其他方式相比，其最大的优势在于不需要了解各种复杂的信息，比如境外银行国际代码、地址等，而只需要收款方的一个visa卡账户就可以了。

目前该业务的合作银行为工商银行，所以需要先成为工行网上银行（u盾或动态口令卡）客户，而收款人只需拥有全球任一visa卡账户即可。

用西联汇款或速汇金即时到账。如果急于在最短时间内将款项转入境外账户，可借助西联汇款渠道，但很贵。目前专业汇款公司纷纷和国内银行合作，推出了一系列的跨国汇款服务，如与农业银行、邮局合作的西联汇款，与工商银行合作的速汇金汇款等。速汇金到账一般只需10分钟左右，而西联汇款也只需要15分钟左右，它们免收钞转汇费用、中间银行手续费和电报费，只按照相应的汇款金额所属等级一次性收取手续费。

目前，西联汇款与多家银行合作，开发了网上银行发出西联汇款的通道。西联汇款是国际汇款公司（Western Union）的简称，是世界上领先的特快汇款公司，迄今已有150年的历史，它拥有全球最大、最先进的电子汇兑金融网络，代理网点遍布全球近200个国家和地区。西联汇款公司是美国财富500强之一的第一数据公司（FDC）的子公司。汇款人可以通过银行个人网银寄出汇款。办理时，汇款人需要先填写“发汇表格”，在递交表格、汇款、手续费及个人身份证件后，会收到一张印有汇款监控号码（mtcn）的收据。凭此号码，可在网上跟踪汇款状态。当然，也需要将汇款信息，特别是这个汇款监控号码告知收款人，以便其领取汇款。

尽管随着技术的进步与第三方支付的渗透，跨境汇款方面的便利性与以往相比有了一定程

度的提高，但是，大多情况下，人们在办理跨境汇款业务时，还是要受到各种条件限制，如需要提供相关的证明和缴纳高昂的手续费。可以说，现阶段，跨境汇款提供的服务还不能很好满足人们的需要。那么，是什么导致了跨境汇款的诸多问题，何时才能享受到方便、快捷与低廉的跨境支付服务呢？

2. 跨境汇款的烦恼

提到跨境汇款，最绕不开的就是SWIFT。每天通过SWIFT网络进行的支付委托超过6万亿美元，有210个国家的逾1万家金融机构参与交易。众所周知，电汇是最常用的国际汇款方式，其中，国际汇款的电文通常用SWIFT制定的标准方式发送。SWIFT是跨国转账的高额“电讯费”的真正收费者。

SWIFT是国际银行同业间的国际合作组织，成立于1973年，总部设在比利时的布鲁塞尔，目前全球大多数国家的大多数银行已使用SWIFT系统。同时在荷兰阿姆斯特丹和美国纽约分别设立交换中心（Swifiting Center），并为各参加国开设集线中心（National Concentration），为国际金融业务提供快捷、准确、优良的服务。通过SWIFT网络，一个位于中国的银行使用电子化手段可以和一个位于纽约的机构之间进行客户信息交换、银行间资金清算、支票清算、共享余额或证券交易等信息。SWIFT的使用为银行的结算提供了安全、可靠、快捷、标准化、自动化的通信业务，从而大大提高了银行的结算速度。

SWIFT运营着世界级的金融电文网络，银行和其他金融机构通过它与同业交换电文（Message）完成金融交易。中国是SWIFT会员国，中国银行、中国工商银行、中国农业银行、中国建设银行、中国交通银行等均加入了SWIFT组织，开通了SWIFT网络系统。

SWIFT自投入运行以来，在促进世界贸易的发展，加速全球范围内的货币流通和国际金融结算，促进国际金融业务的现代化和规范化方面发挥了积极的作用。SWIFT的设计能力是每天传输1100万条电文，而当前每日传送500万条电文，这些电文划拨的资金以万亿美元计，它依靠的便是其提供的240种以上电文标准。SWIFT的电文标准格式已经成为国际银行间数据交换的标准语言。这里面用于区分各家银行的代码就是“SWIFT Code”，依靠“SWIFT Code”就能将相应的款项准确地汇入指定的银行。

尽管SWIFT在跨境汇款方面发挥了基础性的作用，但是其高昂的手续费常常备受诟病。不仅如此，需要在特定的时间办理跨境汇款业务、输入各类信息、烦琐的办理手续以及较长的汇款时间严重影响了客户的体验。同时SWIFT还面临着安全问题，包括支付风险和系统风险。

可以说高昂的手续费和漫长的转账周期一直是跨境支付的痛点。一是延时问题。在跨境汇款时，首先需要经过代理行建立关系，比如欧洲的代理行还要通过欧洲SEPA转账系统进行转账。中间方之间需要相互建立信用关系。由于中间代理层级多就产生了延时问题，跨境汇款经

常需要2~3个工作日的时间，资金的流动性由于延时大幅度下降。二是费用问题。汇款费用贵的原因在于基础设施方面：固定费用、金融伙伴、审核制度、全球机构和运行一个全球的支付网络。不可忽视的是，不透明也是费用过高的重要因素，因为不透明降低了同行的竞争。此外跨境汇款的每一个环节都要收费。例如SWIFT会对通过其系统进行的电文交换收取较高的电讯费，在我国通过中国银行进行跨境汇款会被收取单笔150元的电讯费。三是风险问题。比如中国的银行把钱支付出去，美国的银行违约倒闭了，就会导致中国的银行连带出现问题。四是不利于反洗钱和反恐的要求。由于中间经过的人太多，资金流动增加了不确定性和隐匿性，也增加了监管的难度。

在2012年，全球总共的汇款额达到了5340亿美元，年增长率为8%。事实上，汇款是世界上最贵的一种支付形式，在2013年的第一季度汇款所产生的费用占比为9.05%。金融汇款操作员们从转账费用、外汇转换的手续费、服务费和各种名目繁多的收费中获得巨额利润。在2012年，世界上最大的汇款机构西联汇款净赚取了10.2亿美元的利润。这些费用对任何人来说都是很高的，尤其对低收入人群会造成更大的压力。世界银行曾经评价：“如果汇款的手续费降低5个百分点，那么发展中国家每年将会节省超过160亿美元。这些省下来的钱可以用到消费、储蓄、投资当中去。”

犹如天秤的两端，一端是以SWIFT为主体的机构和银行，另一端是个人用户。不管用户对于跨境转账的抱怨有多少，SWIFT仍旧可以丝毫不予理会，因为天秤永远不会偏向用户。

但是基于区块链或分布式网络技术即将改变这一格局。在区块链技术去中心化的机制下，用户能以更低的费用和更快的速度完成跨境转账，它的出现似乎与人们的期待不谋而合。生活在互联网上的人们，呼唤着快捷、方便与随心所欲，厌恶复杂、迟钝和昂贵，早已经厌烦某些组织的“规定动作”，迫不及待地想开始新的尝试，一场新的支付革命呼之欲出。

3. 为什么是Ripple

“春江水暖鸭先知”，最先引起警觉的便是风投机构。与此同时，区块链技术在国际汇款上的应用已经引起了各国的关注。越来越多的大型金融机构开始尝试，使用区块链技术进行跨境业务结算。2015年，伦敦交易所、法国兴业银行（Société Générale）和瑞银集团（UBS, United Bank of Switzerland）已经开始探索区块链在该跨境汇款方面的应用。韩国和区块链的相关事件也逐渐增多。除了2015年底韩国新韩银行参与区块链企业的融资之外，韩国央行在2016年1月的报告中也提出鼓励探索区块链技术。韩国国民银行（KB Kookmin Bank）正在开发基于区块链技术的国际汇款解决方案，目标是引入“更安全、更快”的外汇服务。另据报道，Visa欧洲公司宣布它正在开发基于区块链的汇款服务。其目的是可以为发送方和支付接收方制定出更完备的汇款服务，包括费用、交易速度和使用便捷性。除了摩根和Visa之外，瑞穗金融集团也开始投入这一领域。瑞穗的区块链项目还包括与微软日本、区块链初创企业Currency

Port及

ISID (Information Services International-Dentsu) 合作银团贷款系统开发。菲律宾已经开始用比特币驱动的汇款服务，为该国海外公民向家乡汇款提供服务。据悉，将比特币技术应用在国际支付的业务上能够为整个银行业节约150亿~200亿美元的交易成本。利用区块链技术布局跨境汇款业务已经成为大型金融机构抢先布局的阵地。

近年来，支付领域的创新不断，尤其是第三方支付的发展使得人们重新审视科技给予生活的便利。中国央行原副行长吴晓灵曾指出，分布式跨境支付用信息技术构建价值传导网络是值得探讨的方向。在国际汇款及跨境支付上，虚拟货币有其天然的优势。虚拟货币全球流通，不受地域限制，实实在在解决了在效率和成本上的问题，尤其在小额支付领域也被认为有非常大的潜力。

在跨境汇款实践方面，不得不提到的是Ripple。Ripple成立于2012年，致力于建立一个去中心化的全球汇款系统。截至2015年10月，该公司的A轮投资已经达到3200万美元。Ripple支付协议利用去中心化的支付清算协议致力于挑战目前全球银行已经通用的SWIFT协议。那么，Ripple为什么能够获得资本的青睐？Ripple和瑞波币又是什么关系呢？Ripple支付协议是靠什么来挑战SWIFT协议的呢？

在Ripple网络发展的早期，其用户一直不多，仅流行于若干个孤立的小圈子，原因是Ripple协议的最初设计思路是基于熟人关系网和信任链的。一个人要使用Ripple网络进行汇款或借贷，前提是网络中的收款人与付款人必须是朋友（互相建立了信任关系），或者有共同的朋友（经过朋友的传递形成信任链），否则无法在该用户与其他用户之间建立信任链，转账无法进行。2013年，Ripple Labs成立并开始搭建代表“未来支付”的平台。在这个平台上，Ripple网络引入两个机制来解决孤立小圈子的问题。

其一是推出瑞波币，它作为Ripple网络的基础货币，就像比特币一样可以在整个Ripple网络中自由流通，而不必局限于熟人圈子。瑞波币是一个网络内的工具，它有两个作用，一是防止垃圾请求攻击（由于Ripple协议的开源性，恶意攻击者可以制造大量的“垃圾账目”，导致网络瘫痪。为了避免这种情况，Ripple Labs要求每个Ripple账户都至少有20个瑞波币，每进行一次交易，就会销毁十万分之一个瑞波币。这一费用对于正常交易者来说成本几乎可以忽略不计，但对于恶意攻击、制造海量的虚假账户和交易信息者，所销毁的瑞波币会呈几何级数增长，成本将是巨大的）；二是作为桥梁货币，成为各种货币兑换的中间物。

其二是引入网关（Gateway）系统，网关是Ripple网络中资金进出的大门，它类似于货币存取和兑换机构，允许人们把法定货币、虚拟货币注入或抽离Ripple网络，并可充当支付双方的桥梁，即作为陌生人之间的“共同朋友”，相当于SWIFT协议中的银行，这使得瑞波币之外的转账可以在陌生人之间进行。

瑞波币是2013年引入Ripple系统的，瑞波币的存在相当于是Ripple系统的润滑剂和桥梁，为

Ripple系统的流动性提供了巨大的便利，从而带动了Ripple系统的发展。但是，Ripple系统中最重要的不是瑞波币，而是Ripple支付协议。

相比比特币，瑞波币更透明一些，没有涨跌风险，交易速度更快。比特币的交易一般需要至少10分钟才能确认，而瑞波币确认只需要5秒。未来还有可能支持所有虚拟货币，且由Ripple网络自动进行汇率换算。

Ripple支持任何货币，而且它还能让用户随意选择货币：用户可以选择持有一种货币，但使用另一种货币支付。在Ripple之中用户可以持有美元，同时以日元、欧元、比特币、黄金以及其他任何货币向商家进行支付。Ripple网络通过在大量争相赚取差价的做市商之间传递兑换单的方法来进行货币“兑换”。

Ripple的分布式外汇交易可以让用户无须中间人，也无须其他兑换所就能完成交易。任何人都可以在全球的订单池中输入买单或卖单，而Ripple network会找到最有效的途径来撮合交易。无须网络费用，也没有最低数额限制。

网关作为Ripple支付系统之中的节点，在支付和转账过程中起到了举足轻重的作用，目前，中国国内已经发展了几个比较大型的Ripple网关，在全世界公开的21家Ripple网关中，中国占三家，它们分别是Ripple China、Ripple CN、Ripple Fox。目前Ripple Fox的发展最为迅速。

2014年，Ripple实验室宣布德国Fidor银行成为首家接入Ripple协议的银行，这意味着瑞波币开始被金融机构接受。但是，可以说Ripple的颠覆之路走得并不顺畅。2015年底，Ripple关闭了在线钱包服务，逐渐将重点转移到B2C业务。仅仅2015年，Ripple就与苏格兰皇家银行、西太平洋银行、澳新银行、澳大利亚联邦银行等多家银行达成合作，此举或许是策略的调整，将重心转移至全力为银行提供基础设施技术。虽然有了起步，但新生代要“征服”银行，仍是任重道远。

与Ripple自己建立了一套类似去中心化的技术系统不同，近年来诞生的如Align Commerce、Bitwage和Abra等公司，主要是基于区块链技术，以比特币充当货币媒介来实现整个汇款流程。这些公司获得了资本的青睐，是跨境汇款的先行者。但是，这三家公司面临比特币价格波动的风险，即在汇款期间比特币价格发生变动从而影响货币的正常兑换。Abra是通过生成智能合约交由一个对手方来套期保值。Align则声称有很多交易所合作伙伴，比特币价格波动对其影响不大，但是如果兑换量过大，还是难免对比特币的价格产生冲击。因此，这类平台的业务发展将在一定程度上受制于比特币交易的规模，需要进行比较复杂的比特币交易设计。

另外一家令人瞩目的则是中国的OKcoin，该公司成立于2013年，目前是国内最大的比特币交易平台。币行是OKCoin公司旗下的重要产品之一，是方便易用的比特币—法币超级钱包，是建立在开放的比特币网络上的开放的钱包、支付、清算、结算产品。币行钱包能够大大降低支

付和汇款的手续费成本，提升效率，带来比特币交易的极速体验。除了提供实时、免费的跨国汇款服务之外，还提供比特币买卖，比特币保险柜等功能，增强了比特币的投资，方便了用户和商户的使用。

4. 未来还将发生什么

以比特币为代表的数字货币，并非是人民币等法币的直接对手，其更类似支付宝一类的支付系统，是对人民币等法币的补充，相当于国际跨界支付的一种中介信用。

建立在去中心化的P2P信用基础之上，虚拟货币超出了国家和地域的局限，在全球互联网市场上，能够发挥出传统金融机构无法替代的高效率、低成本的价值传递的作用。每个人的密码学钱包都可以发展成一个“自金融”平台，它可以进行P2P的支付、存款、转账、换汇、借贷以及全网记账清算，可以通过比特币、以太坊和瑞波币等智能货币系统发行自己的金融合约产品和信用借条。

区块链可以解决跨境汇款成本和效率问题的共同基础是去中心化技术，即交易双方不再需要依赖一个中央系统来负责资金清算并存储所有的交易信息，而是可以基于一个不需要进行信任协调的共识机制直接进行价值转移。建立一个可靠的、中心化的第三方机构需要庞大的服务器成本和维护成本等，一旦受到攻击可能会影响整个系统的安危。而去中心化的方式在节省这些成本的同时，其系统的每个节点均存储了一套完整的数据拷贝，即便多个节点受到攻击也很难影响整体系统的安全。因此对去中心化模式而言，其本身的价值转移成本及安全维护成本都相对较低。但同时需要注意的是，这里的成本仅是针对提供服务的机构而言，如果包含整个基础设施的费用，其社会成本则会急剧上升。尤其值得注意的是，尽管区块链技术确实能够在内部逻辑和运行方式上较好地保障数据安全，但仍难以抵挡黑客对外部设施如用户电子钱包、交易平台等的攻击，且匿名机制使得用户的货币被盗后难以获得法律保障。

除此之外，也面临着政策风险，即政策当局一般会对用户的跨境资金转移进行监管以防范洗钱等行为，而类似区块链技术的匿名机制则为这种行为提供了便利，必然会引起监管当局的关注。

具体到跨境汇款场景，由于其在全球范围内仍缺乏一个低成本的解决方案，不同国家之间还存在文化、政治、宗教等因素的差异，区块链技术这一去中心化、去信任化的模式是一个非常具有吸引力的解决方案，但是具体的技术路线和实践效果仍然有待观察和检验。

区块链将重构股权清算结算

尽管2015年的中国股市又经历了一次大涨大跌，但国民对股票投资的热情还将持续，中国股民数量已超一亿人。随着智能手机和炒股APP的普及，普通股民投资股票越来越便捷，但支持如此庞大数量的股民完成交易的确是一个非常复杂的系统。在每个交易日9：15～15：00的交易时间内，柜台交易系统不断地接收客户的买卖股票的委托，向交易所报盘和从交易所接收成交是否成功的回报信息。柜台系统内部遵照一系列的资金记账原则，例如，买了股票就把客户资金减少，卖了股票就增加客户可用资金，通过调整账户信息记录交易行为。但是，在交易时间内发生的这些资金和证券余额的变动都是临时性质的，必须通过一次“清算”活动，来把当天的所有业务记录到客户账户的余额上，把当天的每笔交易情况归并到历史交易记录中。传统的证券交易需要经过中央结算机构、银行、证券和交易所四大机构之间的协调，才能完成股票交易，效率低、成本高。针对目前资本市场中存在的种种问题，国际各大金融机构开始积极探索区块链应用，包括纳斯达克开发基于区块链的证券发行与交易管理系统；澳洲证券交易所探索利用区块链升级证券结算系统；DTCC、伦敦交易所、芝加哥商品交易所、德意志交易所等机构联合参与“超级账本项目”，等等。那么区块链技术将为证券业带来怎样的一条龙式服务呢？

1. 现实中的证券清算和结算

证券的清算和结算是现代证券交易业务的基础环节，两个环节既相互联系又有所区别。清算业务主要是指对每一营业日中每个证券经营机构成交的证券数量与价款分别予以轧抵，对证券和资金的应收或应付净额进行计算的过程；而结算业务是指证券交易完成后，对买卖双方应收应付的证券和价款进行核定计算，并完成证券由卖方向买方的转移和相对应的资金转移的全过程。由于结算是进行下一轮交易的前提，结算能否顺利进行，直接关系到交易后买卖双方权责关系的了结，从而直接影响交易的正常进行和市场的正常运转。

从国际结算机构的发展历程来看，证券交易平台发展的主要惯例和趋势是交易平台与结算平台前后分离。作为后台，托管与结算业务趋于集中化、一体化；从国际结算方式的发展进程来看，结算方式更加先进，突出电子化、专业化的发展，加强时效性。

目前，我国证券市场已经形成“两所两网”的局面，即上海证券交易所和深圳证券交易所，而且“两所”各自发展，互相竞争。“两网”走向统一，各自的清算登记体系也主要形成了三种模式，即深圳模式、上海模式以及NET与sTAQ模式（法入股模式）。

从我国证券交易的结算机构方面来看，中国证券登记结算公司（以下简称中证登）主要负责上海证券交易所和深圳证券交易所（以下简称交易所）上市公司股票、可转债、基金的登记、托管和结算，作为清算的中央对手方；同时，中证登还负责交易所上市国债、地方政府债、公司债券分托管、交易所场内债券交易的清算，作为其清算的中央对手方。中证登目前主要实行两种交易结算方式为两极结算，其中一级结算主体为投资者与券商，二级结算券商与结算公司。一级结算中：证券交收为T+1开市前，资金交收为当日T+0；二级结算中：证券交收为

T+0收市后至T+1开市前，资金交收为T+1。股票与基金的交易实行T+1的交易方式。即当日买进的证券，要到下一个交易日才能卖出。同时，对资金仍然实行T+0，即当日回笼的资金马上可以使用。但交易所证券结算系统尚未与央行的大额支付系统谅解，资金结算与证券交割无法实现真正意义上的DVP（券款对付）。

目前我国这种证券清算登记制度的不足主要在于“两所两网”各自为政，互相独立，而市场参与者却是共同的。一般的证券商都会同时拥有“两所两网”的交易席位，但交易清算机制又互相独立。因此，加重了券商的成本负担，增加了资金周转风险，不利于券商和投资者在各个市场间的流动，最终会限制全国市场的整体发展。另外，清算登记系统只限于为场内交易提供服务，不注意跨市场、跨地区、跨领域的交收业务的发展，过分依赖场内交易，对清算登记系统的发展不利；只对会员机构服务，不注意对个人客户业务开展，大大降低了清算登记系统的效率。而且，资金清算依赖于银行体系，尤其是人民银行电子联行系统。因此，银行系统的效率直接影响证券市场资金交收效率。

2. “交易即结算”——区块链为证券市场带来的新变革

高成本、低效率一直是全球证券股权交易的问题所在，而作为一种数字化，安全防干扰的分布式数据库，区块链不仅能实现银行业价值安全储存、转移中心的核心功能，又能有效解决目前证券清算与结算的问题所在。由于区块链技术能够为许多金融市场带来庞大的低成本计算能力，让数字资产在交易对手方之间进行转移而不需要任何中央机构来实现交易的特性，全球交易和结算运营者都已经开始对区块链技术的潜力表现出持续增长的兴趣。区块链本质上是一个跨越全球网络的数据库，区块链的产生基于相互独立的网络系统而不是中心化的系统，区块链账本的安全透明、不可篡改、易于跟踪等特点使其可以实现对证券登记、股权管理、证券发行进行数字化管理，且变得更加高效和安全。在传统的IPO（上市）流程中，需要先审核，再负责发行和交易。由于区块链使用了先进的计算机加密技术来跟踪交易，它在证券结算清算系统中能够省略清算所、审计员去验证交易的步骤，不再需要托管人员去验证投资者股票持有的真实性。从本质上看，这是在证券结算与清算的过程中“去中心化”，在交易系统中省略了中间人和后台，降低了第三方审计、记账和验证交易的高额成本，从而降低了证券交易所的交易成本。此外，点对点交易也意味着清算过程可以实时发生，与传统“T+3”和“T+2”的清算时间相比，区块链技术提高了资产的流动性，让交易者持有股票等同于手持现金，而资产的高流动性也意味着证券交易能够吸收更多的股票投资。区块链技术还带来了高透明度的权益市场，由于每个交易参与者都有完整的交易记录，伪造交易或者篡改交易记录的行为几乎不可能实现。如果发生虚假交易或是篡改交易，参与交易的交易者会发现账本记录中出现不同，然后拒绝进行交易。区块链技术也为增加证券发行的灵活性创造了条件，利用区块链技术生成的智能合约，在最理想的情况下，可以实现任何人以自己任意设定的方式自行发行资产凭证，通过区块链实现24小时不间断运作，所有人都可以在去中心化的交易平台上自由竞价完成交易，而撮合也是去中心化的，“交易即结算”在区块链体系中变得非常现实。此外，区块链是一种分布式的

总账，这也意味着所有使用它的人都可以维护它，而不是通过一个中心化的计算机，从理论上而言，这使得区块链系统比中心化的总账更为安全，其维护也更为经济。

我们可以从如下两个图来看运用区块链技术后，证券结算与清算系统会有怎样的变化。图3-2是美股中典型的“T+3”结算方式，也就是交易发生后第三个工作日才能完成清算交割。在传统证券交易中，证券所有人发出交易指令后，指令需要依次经过证券经纪人、资产托管人、中央银行和中央登记机构这四大机构的协调，才能完成交易。整个流程效率低、成本高，且这样的模式造就了强势中介，金融消费者的权利往往得不到保障。据估算，美国两大证券交易所每年所需清算和结算的费用高达650亿~850亿美元，但如果将“T+3”天缩短一天为“T+2”，每年费用将减少27亿美元。

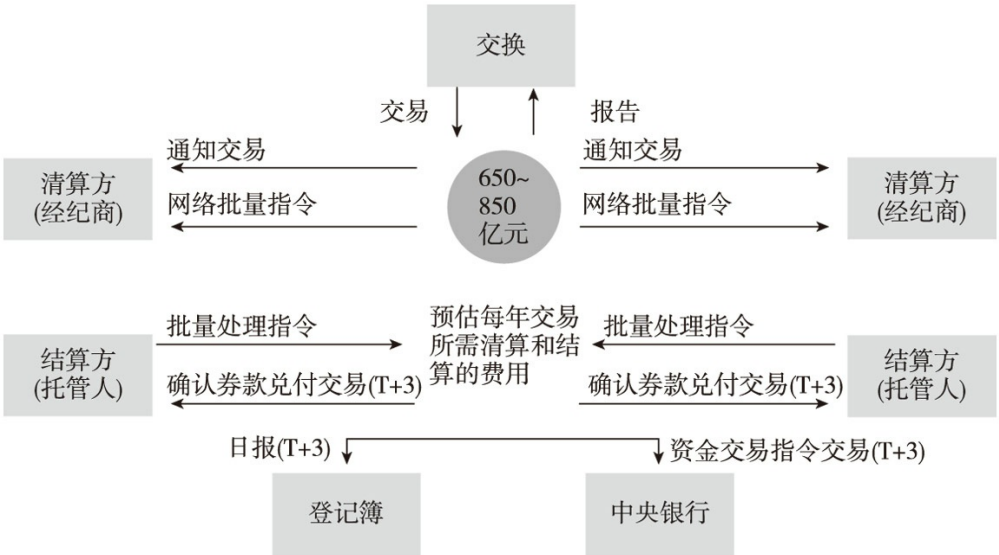


图3-2 证券结算和清算系统中典型的“T+3”

资料来源：巴比特

而利用区块链技术改善的证券交易结算系统会怎样呢？如图3-3所示，买卖双方能够以智能合约直接实现自动配对，并通过分布式的数字化登记系统自动实现清算结算。这就意味着没有中央记账系统参与，而是通过每个参与者将发生的每笔交易记录下来的方式确认交易。由于区块链数据不可撤销且能够在短时间内将数据拷贝至每个数据块中，真实的交易信息能够快速、准确地区块链上产生公示，证券交易的买方和卖方、交易股票数目、股价、交易时间和资金的结算都会被真实记录下来，交易的发生和所有权的确认不会再产生争议。与以往交易确认需要“T+3”天不同，区块链上结算和清算的完成仅需十分钟，这种去中介化的交易流程毫无疑问将大幅节省交易费用和管理成本。

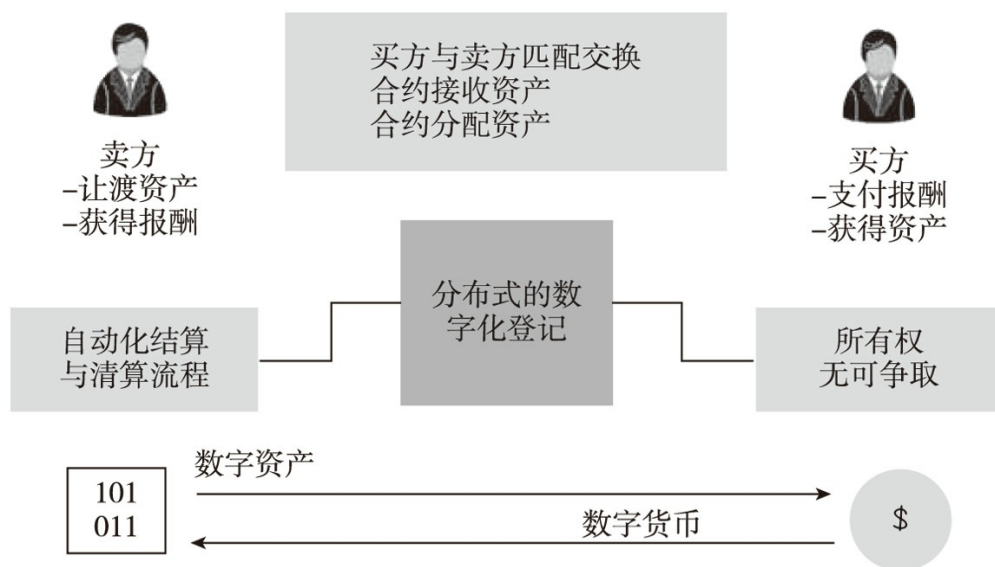


图3-3 区块链应用于证券结算和清算系统

资料来源：巴比特

3. 已经开始起跑的Overstock、纳斯达克和澳交所

如果说最早做区块链证券项目的公司，大概要属美国在线零售商Overstock了，这家公司曾经和创业公司Counterparty合作共同开发了一个名为美第奇（Medici）的项目，后来因为种种原因，美第奇项目没有开发成功，但双方推动区块链技术在证券市场应用的努力却没有停止。在此之后Counterparty与MathMoney f(x) 公司合作开发了瞄准证券市场的symbiont.io，而Overstock也继续开发自己的区块链项目并在2015年4月率先公布了名为tØ的部分项目信息，该平台的目标是基于区块链技术实现股权的交易和结算功能，发挥区块链“交易即是结算”的优势。2015年6月，Overstock进一步宣布将采用彩色币的形式发行一种“数字企业债券”或者也可称之为“数字加密证券”，债券的总价值约为2500万美元，并将其作为美第奇项目的一部分内容，这种加密证券将通过TØ.com平台发行。2015年8月，Overstock在纳斯达克的一次活动上正式推出了区块链交易平台项目tØ，设计目标是基于区块链技术建立可实现证券交易的实时清算结算功能的全新系统，该系统同时包括了证券的发行功能，同时宣称Overstock已经基于该系统进行了私募债券发行的尝试。按照美国证券监管机构的相关规定，发行私募债券并不需要监管机构的批准，但这一监管豁免仅限于私募领域，公募证券的发行需要得到美国证券交易委员会

（SEC）的批准。随后，Overstock向SEC提交了S-3申请，并最终获得了SEC的批准。S-3是一种证券发行的登记表，可以让企业在获得监管当局认可的前提下以一种更为简化的方式发行证券。Overstock的申请获得SEC的批准，意味着这家公司可以用同样的方式来发行公开交易证券，这也是美国监管部门首次公开批准基于区块链技术开展此类业务，也许这将是今后证券发行和交易方式改变的开始。基于tØ平台的发布和来自SEC的批准，Overstock计划完成价值高达5亿美元的股票或其他证券的发行，发行产品包括普通股、优先股、存托凭证、权证、债券等。

仅仅在Overstock推出tØ平台两个月之后，2015年10月底，纳斯达克宣布要推出基于区块链技术而建立的新平台Linq，该平台以在私募证券市场建立一种全新的股票发行、转让和出售方式为目标，将可能彻底改变资本市场基础设施系统的核心，尤其是对于交易结算和行政审批等过时的管理功能的颠覆。现实中初创公司往往希望在一定时间之内保持非公众公司的身份，而暂不进行公开发行，因为投资者希望在早期阶段减少来自外界的压力而获得一定的独立性。基于这种考虑，初创公司想要获得一定的流动性就需要通过私募发行获得一定的融资。在传统私募市场中，初创公司在处理股份交易时，需要大量手工作业和基于纸张的工作，例如需要通过人工处理纸质股票凭证和期权发放等工作，需要律师手动验证电子表格等，而这些工作不仅需要大量人力物力成本，还可能因很多人为因素造成错误。此外，私募规模往往较公募更小，不论从融资成本的角度还是保守商业机密的角度来说，初创企业都不愿通过大量外包进行融资。许多企业在寻求股份管理特别是私募股份管理的有效解决方案，而纳斯达克的Linq平台在这个领域为市场提供了一个全新的选择。

Linq由纳斯达克内部的技术开发人员与区块链创业公司Chain公司共同创建，开发当中也得到了全球设计和创新公司Ideo的技术支持，Linq的服务将覆盖初创企业证券的发行、交易和登记管理各项功能。Linq基于区块链技术开发，其在股权市场的应用可以移除私募股权市场对纸笔或者基于电子表格的记录保存的需求，为用户提供一种不可篡改、永久保存的记录，兼具透明度和可审计性，这是此项技术拥有的最大优势。这种架构也允许用户迅速完成转换所有权，进一步降低了对对手方违约或遭到第三方操纵的风险，证券业长久以来梦寐以求的“即时交割”目标有望实现。Linq被市场看好的另外一个原因在于，纳斯达克拥有较其他公司更为丰富的为股权服务的配套系统。目前纳斯达克私人股票市场已经实现了基于云的股票管理解决方案，可以使私人公司更高效地管理资产和股票计划，而完全电子化、分布式的记账方案Linq使其变得更加高效和安全。2015年12月，Chain公司成功使用Linq平台为新的投资者发行了公司的股权，成为第一家使用Linq来完成并记录私募证券交易的公司，而纳斯达克也减少了结算时间。此外，上线Linq平台的几家初创公司还包括ChangeTip、PeerNova、SYNACK、Tango和Vera。

2016年初纳斯达克还宣布正在研发一种基于区块链技术的股东电子投票系统。据纳斯达克相关代表透露，将会选择爱沙尼亚纳斯达克OMX塔林证券交易所作为试点进行试验。而纳斯达克也仅仅是瞄准私募股权市场的参与者之一，2015年8月，Symbiont对外宣布它已通过分布式总账技术发行了自己的股票。

据澳洲媒体SMH报道，澳洲证券交易所（ASX）正在认真考虑使用区块链技术作为其清算和结算系统的升级方案。ASX已经认购了区块链技术开发商DAH公司的1500万美元股份，主要目的就是为优先使用区块链技术升级ASX的股票系统，DAH将与纳斯达克一起为澳大利亚证券市场设计结算系统。ASX首席执行官Elmer Funke Kupper（埃蒙·弗克·库珀）表示，该证券交易所正在替换其交易系统，因为区块链能够降低清算和结算交易的成本和复杂性，并能节省交易时间。而此前的这些工作，都是由清算所电子附属登记系统（CHESS）来完成的。

ASX正在寻求新技术以提高终端之间的效率，大量削减来自投资银行和交易后端的管理成本，而这正是区块链的潜力所在。升级ASX的证券结算系统将会从2016年底开始，大约需要近5年的时间来完成。ASX应用分布式账簿系统的计划分为两个阶段，第一阶段的主要目标是实现该技术的应用，并测试分布式账簿技术能否应对澳大利亚股票市场这样大规模的应用场景，这在监管层面来看已经涉及重大国家风险管理的基础设施。此外，澳大利亚政府也将对区块链是否适合在证券清算行为上应用进行评估，如果可行，ASX将会积极推进研究。

4. 改进的空间

区块链技术的应用有望在证券交易上实现实时结算和清算，那么这对于证券交易是否就是完美的解决方案呢？能够提高资产的流动性显然是极佳的，现在许多金融机构都在投资区块链技术，力求降低清算及结算成本，加速清算程序。比如在证券交易上能够最终达到“T+0”也就是当天结算实时清算，而不是现在的两天和三天之后。但是Tabb Group研究所的创始人Larry Tabb认为当前基于共识算法的区块链技术应用与当今市场操作有很多不可兼容性，主要表现为如下四个方面。

（1）对融资融券模式造成很大影响

大部分的投资机构允许他们的托管人或经纪人向投资者借贷他们的“闲散”证券去填平空仓。当拥有可贷证券的投资者决定卖出这些证券时，必须解约借贷程序，这意味着在销售完成结算前，证券必须退回至投资方的账户之中。鉴于目前欧洲清算时间是“T+2”，美国是“T+3”，托管人和经纪人具有足够的时间将证券退回给投资方。而如果变为基于区块链的“T+0”系统，就意味着必须在销售发生前或销售发生时实时向投资者退还借出的证券。如果不能实现上述操作，那么投资者不得不持有降价股票，直到借出的证券返回他们的账户，然后他们才可以执行瞬时结算交易。除此之外，在这个过程中，可能会产生信息泄露问题，大家可以知晓哪些借出证券的投资者正在寻找出售证券。

（2）泄露客户交易信息

在美国，金融工具不是登记在它们的持有者名下，而是在交易记录系统之下，例如信托托管和结算公司。存管方不知道他存管的证券是属于谁的，但只知道哪位托管方或股票经纪人持有哪些证券，而后者知道哪位客户持有这些金融工具。如果转向基于区块链的系统，由于其中清算是瞬时完成且不能改变交易的，因此在交易发生时或之前，系统必须知道客户的姓名，这也可能会导致信息泄露，对于大型投资者来说，这是个严重的问题。因为很多投资者都不想让他们其他投资者知道他是什么仓位。这样会将现在的匿名市场变为公开市场，从很大程度上改变市场参与方的行为方式。

（3）造成交易冲突

同一家机构的不同投资组合经理通常会整合同一种证券的订单，然后放入市场的单一交易块中，以降低价格波动和交易费用。如果使用区块链，这些交易块的操作将变得比较困难，因为区块链是一个资产所有权记录，从技术上来说，投资者购买的证券不是投资机构的资产组合，而是投资经理所管理的单一资产。因此，每位资产组合经理必须单独执行，而不是在大型交易块中操作。这就意味着，同一家公司的资产组合经理们会在同一时间下单，事实上他们是在争夺流动资产，一家大型金融机构可能会在市场中进行内部争斗。

（4）无法实施净额结算

净额结算可以在投资机构内部实现部分清算工作，最终会降低清算成本。在T+0环境中，每笔交易都需要瞬时结算，这样就会增加交易量，仅是美国权益市场，每天的交易量将会达到290万笔，使用目前的公共比特币区块链，需要超过一个月的时间来处理目前一天的交易量，这样基于区块链的交易系统将面临延时较大、吞吐量较小的问题。

尽管从大方向来看，基于区块链技术的系统可以改善证券交易系统，但类似会计和风险计算，这些通常需要拥有强大计算能力的后台核心系统完成的功能很可能在区块链技术方面会受到一些“限制”。而且将区块链技术应用到清算系统中，也需要引入一种新型费用。在比特币中，矿工们运行比特币交易，解决最优化问题，然后获得新创造的比特币奖励，同时希望完成交易的比特币用户也为他们支付清算费用。矿工根据费用高低和区块上交易记录问题的困难程度，为交易优先排序。区块链不需要中央清算所，但仍可将后台运行维护的费用转嫁至投资者身上，最坏的一种情况是投资者之间将结合付费展开交易顺序竞争，每个人都有支付较高的费用力争他们的交易比其他投资者更快完成清算的意愿。

股权众筹——基于区块链技术的畅想

虚拟现实技术最近甚嚣尘上，有人预言它将颠覆传统电子游戏和游戏体验。2012年，还是一家创业公司的Oculus VR开发了一款为电子游戏设计的头戴显示器Oculus Rift，这是一款虚拟现实设备。Oculus VR公司在2012年8月将Oculus Rift在Kickstarter众筹网站上发布，计划融资250万美元，但出乎其意料的是首轮融资就超募达1600万美元。2014年3月Oculus VR创始人以20亿美元的价格将其卖给了Facebook，但参与众筹的人却只得到了一件T恤作为投资回报。上述例子很好地反映了众筹这一新兴商业模式的两面性：一方面，众筹平台可以通过“预收+团购”的形式提前使创业者获取市场对创新产品的反馈，如果市场反应良好，就像Oculus Rift公司之前的经历一样，你可能要做好“成功正在向你走来”这样的准备，你的企业将会获得巨大的估值，这是众筹的威力；另一方面，作为众筹项目的投资者，尽管你的商业判断得到了市场的承认，但你获得的可能只是一件装备或者来自创业者的一个签名，你只是这次成功的旁观者，从这个角度

讲，众筹的意义对你来说并不是非常显著。但现在区块链技术的创业者希望通过区块链技术去中心化、高透明度又不可篡改的交易记录特性为众筹商业模式带来一些实质性的变革。那么，众筹将如何发展，区块链技术又将如何和众筹相结合赋予其更大的创新能力呢？

1. 不可忽视的众筹

一直以来，资金就是创意想法以及创业事业面前的一道鸿沟，也正是这个鸿沟催生了世界上第一家众筹平台。互联网众筹模式的鼻祖Kickstarter的诞生即源于一位华裔创始人Perry Chen（陈佩里）。陈佩里的正式职业是期货交易员，但其非常热爱艺术，他开办了一家画廊，还时常参与主办一些音乐会。2002年，陈佩里曾因为资金问题而被迫取消了一场已经在筹划进展中的音乐会，这让他非常失落。由于资金问题而导致音乐会的无法开展让陈佩里认真思考如何解决募集资金的问题。2009年4月Kickstarter终于上线了，在不到10年的时间里，Kickstarter已经成为目前世界上最大的两个互联网众筹平台之一。

Kickstarter的运作方式是一种典型的平台商业模式，该平台的用户一方是渴望进行创作和创造的人，另一方则是拥有部分资金并愿意对新的创意提供资助的人，双方共同的愿望都是希望新的创意变成现实，并能实现持续推广。Kickstarter网站的创意性活动包括13类，基本都是和人的日常生活直接相关的领域，例如电影、音乐、美术、摄影、戏剧、设计、技术、食品等。在Kickstarter上，任何人都可以向某个项目捐赠特定数目的资金，网站收取很低的佣金。Kickstarter主要进行的是商品众筹，也就是利用互联网和社交网站的传播特性，让小企业、艺术家或个人向公众展示他们的创意，争取大家的关注和支持，通过“团购+预购”的形式，向网友募集项目资金的模式。相对于传统融资方式，商品众筹更加开放，筹资人能否获得所需资金主要是看投资人对项目创意的认可程度。从市场营销专业的角度来说，在商品或者项目诞生之前就已经接受了一次市场的投票，那么商品的市场前景无疑将会获得更为准确的验证。因此，可以说只要是网友喜欢的项目，只要是有了投资人的认可，都可以通过众筹方式获得项目启动的第一桶金，为更多小本经营或创作人提供了获得成功的第一步台阶。

在Kickstarter上，大部分的众筹项目中的投资者都可以获取相应回报，可能是一封感谢信或是制作完成的产品，这都基于参与者赞助的资金金额。在现有的众筹商业模式中，商品众筹和股权众筹是相互分离的，商品众筹的参与者往往只能获得实物回报而不能持有这些项目的股权，而股权投资者可以获得一定比例股份回报。2015年一部动画片《大圣归来》火爆银屏，片尾滚动着的89位投资者的名字成为影迷们津津乐道的另一个热门话题。《大圣归来》出品人路伟早年从事金融行业，转而选择影视行业开始创业之后，《大圣归来》是其第一个项目，对金融产品非常熟悉的路伟通过众筹合计募资780万元，当票房超过5亿元之后，项目整体投资回报率已经高达400%，路伟与全体投资人总共获得收入3000多万元，平均每位投资者可以净赚近25万元。《大圣归来》创造了中国电影众筹史上的第一次成功。2015年5月29日，wifi万能钥匙在“筹道”股权众筹平台上线，项目上线不到一个小时，浏览量即突破10万，截至2015年6月10日

众筹成功时，浏览量已超过300万，共有5712人认购，认购金额达到70亿。吸引到如此多的投资人和民间资本，wifi万能钥匙确实做到前无古人，原本只属于专业投资机构通过股权投资获得收益的机会，因为股权众筹的出现使得普通人也能参与其中，股权众筹在为广大投资人提供投资机会的同时也体现出了超乎寻常的成就梦想的實力。

客观来说，股权众筹与投资者在新股IPO时申购股票在本质无太大区别，但在互联网金融领域，股权众筹主要针对的是对初创企业给予的投资支持，在资本市场中可以看作是对天使投资和风险投资的有力补充。股权众筹具有低门槛、解决初创企业融资难、依靠大众力量推动社会创新创业发展等特征。我国股权众筹行业在2015年得到迅速发展，中国平安、京东、阿里等实力雄厚的互联网公司纷纷宣布成立股权众筹平台。2015年3月31日，京东推出股权众筹平台，同一天，平安集团的股权众筹平台也完成了工商登记；5月19日，蚂蚁金服宣布将筹备上线股权众筹平台，命名为“蚂蚁达客”。此外，天使汇、众筹客等平台早已建立了明确的商业模式，更有众多成功案例。据中关村互联网金融研究院监测数据显示，2015年我国股权众筹行业成交规模快速增长，截至2015年11月，该机构监测的78家平台累计成交量达141.2亿元，充分表明股权众筹这一商业模式获得了投资人和创业者的认可和接受。据业内人士预计，伴随着国内相关监管法规的出台，股权众筹行业将迎来更为规范的发展，该市场未来发展空间巨大，将达到千亿元人民币。世界银行预测，到2025年全球发展中国家的众筹投资将达到960亿美元，中国有望达到460亿~500亿美元，而这其中，约70%~80%的融资额将是股权众筹融资。

2. 基于区块链技术的众筹平台畅想

Kickstarter、Indiegogo和其他所有的传统众筹平台作为第三方平台，促成一项众筹活动的流程大概是：为项目展示提供平台，对项目发起方的基本资料进行尽职调查，如果投资人对展示项目感兴趣，项目支持先将资金转到众筹平台账户，当项目筹集的资金达到目标数量时，平台将资金转到项目发起人账户，或者项目筹集的资金没有达到目标数量，发起项目失败，平台将资金返还给投资者，投资者获得的回报是预订项目产品的权利或者是公司股权。

区块链是一种创新的分布式交易验证和数据共享技术。它的核心价值在于通过构建点对点的自组织网络、时间有序且不可篡改的密码学账本建立分布式共识机制，从而实现去中心化信任。具体来说，基于区块链的众筹平台可以通过创建自己的数字货币来筹集资金，通过分发自己的“数字股权”给早期支持者，使投资者获得支持初创公司所获股份的凭证。区块链股权众筹平台通常由三层结构组成：最底层为区块链网络，由它构建起一个去中心化信任的分布式总账；中间层为业务逻辑与区块链结合，共同建立账户中心、股权登记、股权凭证、股权交易、股权管理等功能；最上层为各个众筹平台面向客户提供的业务。

从以上区块链技术改善的三方面来看，由区块链技术支持的众筹平台不再需要可信任的第三方中介平台。基于区块链技术的众筹平台允许初创企业通过向早期支持者发行数字货币和售

卖“密码学股份”（cryptographic shares）筹集资金。这意味着参加众筹项目的投资者得到代表初创企业股份的代币（token），可以从代币升值中获得收益，而不只是简单的预定项目产品权利或商品而已。此外，区块链技术能够在股权登记管理、股权转让流通、智能合约等方面为股权众筹带来改变。



图3-4 区块链股权众筹系统架构

资料来源：《区块链：新经济蓝图及导读》

（1）股权登记管理

股权登记是证券交易安全的基本保障。市场经济的基石是财产的确定性，这种确定性是交易的基础。对股权众筹而言也是一样，登记管理极为关键。一方面，登记发挥着向社会展示当事人股权的公示作用，让潜在的交易主体了解特定的权属状态；另一方面，登记也是股权交易的关键环节，记录股权所有者的转移。区块链是用于存储永久性记录的理想解决方案，利用区块链账本安全透明、不可篡改、易于跟踪等特点，记录公司股权及其变更历史具有明显优势。区块链独特的身份账户体系能够将记录的股权作为股权登记的电子凭证。区块链技术能够将现如今大量需要人工处理的纸质版股权凭证和期权的历史交易和维护等进行数字化管理，使其更加高效和安全，通过最大程度降低确权成本对于数量巨大且市值不大的初创企业在股权登记、转让方面具有较大的技术支撑作用。区块链的开源可共享使各个机构和个人均可参与到整个系统的运作，每个参与维护节点都能复制获得一份完整数据库的拷贝，从而对信息的所有者确权。

（2）股权流通转让

对于股权众筹而言，股权流通也是业务中极为重要的一环，能够激发用户的活跃度，促使更多的登记发行。传统的OTC场外股权交易以交易双方的信用为基础，由交易双方自行承担信用风险，需要建立双边授信后才可进行交易，而交易平台集中承担了市场交易者的信用风险。利用区块链技术，股权的所有权登记在区块链中，股权交易必须要所有者的私钥签名才能验证通过，交易确认后，股权的变更也会记录在区块链中，从而保障交易双方的利益。

（3）众筹智能合约

在股权众筹发起初期，由发起人、众筹平台、领投人、保荐人等多方共同签署一份众筹合约，来约定各自的责任与义务。这份合约可以利用区块链技术以智能合约的形式存入区块链中，由区块链确保合约在履行中不得被篡改。

如图3-5所示，根据合约的条件，区块链底层首先产生第一个事务TX1：创建一个联名账户，从领投人账户打款300万到联名账户，并生成200万的借条供投资人购买，该账户由合约中各方共同拥有和维护；同时创建TX2（在规定时间内，如果200万借条销售完，则从联名账户中打款500万到发起人账户中）和TX3（如众筹失败，跟踪联名账户的交易记录，全额退款）。TX1、TX2、TX3在同一时间写入区块链，由区块链底层自动执行。

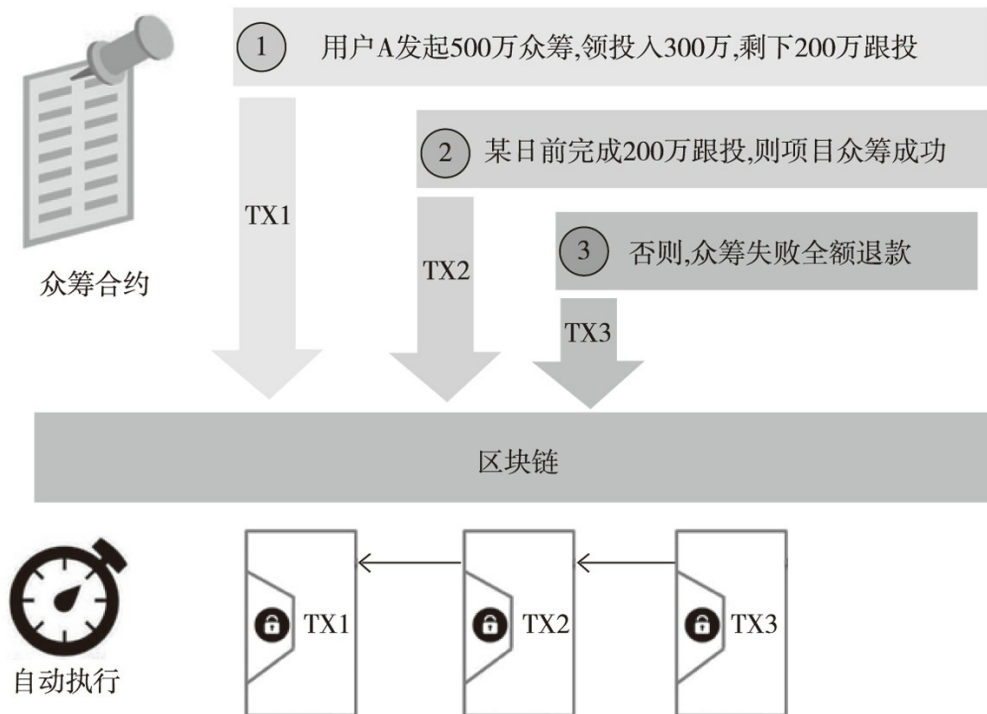


图3-5 区块链众筹智能合约示例

资料来源：《区块链：新经济蓝图及导读》

4. 实践先锋，从Swarm到小蚁

目前，基于区块链构架的众筹平台已经走出畅想阶段，Swarm、Koinify和Lighthouse是三个去中心化的众筹平台，尽管它们的成立没能借助区块链众筹的力量，但是它们已经利用这项技术帮助别的企业成功获得融资。Swarm平台可以说是区块链股权众筹方面的实践先锋。

Swarm被喻为众筹界的Facebook，是世界上首家分布式孵化器众筹，使用比特币技术为底层协议，在这个去中心化的众筹平台上允许初创企业通过发行自有的Coins资产筹集资金。Swarm公司首席运营官Ben Ingram（本·英格姆）将这一平台形容为“众筹界的Facebook”。Swarm团队基于Counterparty平台开发众筹系统，后者是一家基于比特币基础的去中心化技术平台，具有提供交易和创建智能资产等功能。有了Counterparty协议的支持，Swarm平台可以像一个为加密货币投资者建立的社交网络一般高效运转。2015年6月17日，Swarm团队基于Counterparty平台发行“SWARM Coin”标志着这家去中心化众筹平台募集启动资金的开始，也使得投资者们拥有了分享公司未来发展红利的机会。Swarm要求投资与后续回报都得是比特币，公司首席执行官Dietz（戴茨）计划在第一轮融资中也要求只使用数字货币，他认为这应该可以算作是一种内部测试。

Swarm团队的计划是建立一个基于加密数字货币协议的发行平台，用户可以通过财产信息面板等，随时了解自己的资产状况。作为一家逆势成长的创业公司，Swarm肩负的时代任务还有向大众普及“众筹”和“加密货币”两个概念。Swarm团队坚信他们所创建的平台将有助于改变创业者筹资的方式。该公司今后的计划还包括分布式的项目信息调查，即让人们可以参与评估项目，分享相关信息等。

加密货币能为传统众筹方式带来的改变主要有以下三点。第一，以使用比特币技术为基础，不受地区局限。第二，利润不只给参与某具体项目的少数合作者，所有众筹平台的股权投资人都能获得合理收益。假设在Swarm平台上，如果Facebook想要收购通过Swarm平台发行的产品，它必须购买市场上大部分人的股份。这意味着在Swarm参加众筹项目的投资者得到代表初创企业股份的代币（token），可以从代币升值中获得收益。而利用代币这样的加密货币可以确保投资者在众筹项目中获得与投资不断变化的企业价值相符的投资回报。第三，投资人能够通过意见和建议来帮助产品更好地形成和生产，以社区的方式加强沟通。可见，Swarm是建立了一个简单易用的数字加密股份平台应用，投资者可以快速浏览大量市场的“加密股份出价”，有喜欢的就能简单快速买下，而无须经过股票经纪人，达到买卖方便，无安全风险的状态。比如，Swarm目前已通过自身平台募集资金约75万美元，它允许创业者打造数字化的加密货币并分配给投资者。因为代币是虚拟的，创业者可以按照自己的想法为代币赋予价值，比如股息分红、企业发展壮大后的选举决策权、公司相关产品或服务以及任何创造性的投资回报。这些回报都会随着项目的发展程度而增加或减少。相比传统众筹平台，Swarm的创业者可以灵活决定他们对股权的规定。

其他去中心化众筹平台还有Koinify，该平台于2014年9月成立，并从IDG Partners、Brock Pierce的AngelList和zPark获得100万美元风投投资，用于进一步开发去中间化众筹途径运用。该途径将能够完成智能公司（一般也被称为去中间化自治公司，简写DACs）和去中间化运用（DApps）的创立。当Koinify理想的去中间化众筹途径成功确立后，出资者将能运用比特币在Koinify上采购有关各种项目的代币。Koinify主要为与区块链技术和密码学货币相关的项目，如去中心化应用、智能公司等使密码学货币更加容易使用的基础设施筹集资金，想要为去中间化实业获取资金树立一个生态体系，完全创立一个全新的经济基础布局。然而2015年5月Koinify宣布它将不再为去中心化应用提供代币销售平台，将进行转型，但该创业公司并未透露转型计划。其首席执行官TOM DING表示公司对区块链的信念、使用区块链作为底层技术的创新以及尝试重建业务和组织结构等这些公司基本的理念都没有改变。Koinify已经在其博客上通知用户在2015年6月30日之前把他们在GetGems众筹期间购买的代币取出，但仍表示会为已经在Koinify平台上销售软件代币的创业公司继续提供服务。

而在国内，“小蚁”可谓是首家利用区块链数字进行背书的系统。利用区块链技术来登记公司股权可以说是极大的创新，但要在底层逻辑和各种细节上达到我国法律合规并对接实体世界并不容易。在对我国当前法律环境进行深入研究和分析后，“小蚁”很有潜力成为切实可行的区块链应用。目前，“小蚁”系统正在尝试用区块链来登记公司股权（股份），成为公司的股东名册以及持股信息的合法记载场所。

“小蚁”区块链应该说是中国第一个区块链项目，也是国内第一个原创区块链底层协议。“小蚁”的想法形成于2013年底，团队成立于2014年初，“小蚁”是用来发行、管理、交易各种权益份额的区块链协议。初期会以非上市公司的股权作为切入点，为初创公司提供数字化股权激励方案，为股权众筹公司提供股权管理方案，未来会过渡到股权的可交易，即“区块链IPO”，逐步模糊非上市公司和上市公司的界线。

“小蚁”是基于区块链技术，将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化网络协议。可以被用于股权众筹、P2P网贷、数字资产管理、智能合约等领域。众筹完成后，初创公司可以用“小蚁”来管理众多股东的股权，用“小蚁”提供的去中心化交易机制进行股权交易。初创公司获得了市场估值、股权流动性，用户获得了退出机制。通过将股权登记在“小蚁”区块链上，初创公司能够以“区块链IPO”的方式获得资金。

现在大多数比特币支持的众筹平台不为消费者项目筹集资金，只为迎合懂得比特币技术的投资者。尽管这些平台上的项目并非主流，但是仍然值得关注。它们都是基于一个核心原则和范式改变：从中心化的模式转变为去中心化模式，移除中介者的费用和可信任第三方，其中一些项目共享知识产权和自动代理，而不是由大公司独自拥有，专利池由持有某一密码学货币、分布式自治组织或者分布式包裹递送网络的任何人拥有。有了自动代理，可以想象一个自主的

硬件或者软件，它能够通过出售产品和服务，获得比特币或其他密码学货币，并支付自己的成本，存活下去。这种商业模式的好处是服务成本更低，因为它没有许多运营成本，确保了投资者的合理收益，且买卖方便。

另外在股权众筹融资方面，区块链技术能够为各方带来更加公开透明和真实可信的信息，且信息对投融资各方更加对称，记录难以篡改、伪造、消除。它为去中心化比特币生态系统——无论是基于货币的比特币或者是基于比特币协议的不同应用如核心开发筹集资金等，都提供了一种新方式。

票据业务——依托区块链平台的改造

2016年1月，中国农业银行北京分行爆发票据窝案，38亿元无法兑付。事件的主要经过是中国农业银行北京分行2名员工利用非法套取的票据进行回购资金，且未建立台账，回购款中相当部分资金违规流入股市，由于股价下跌，出现巨额资金缺口无法兑付。该事件简单来说就是：A银行以买入返售的方式与B银行做了一笔票据转贴现业务，按照规定，纸票本应在回购到期前，存放在A银行库里，不得擅自转出。但事实上，纸票在回购到期前，已被票据中介取出，卖给了C银行。买入返售到期后，钱并没有回到账上，而库中的票据则被换成报纸放在库里。在这个案件之后我们尝试设想另外一种情况，如果票据贴现的资金只能回到农业银行北京分行的账上，这一损失是否可以避免？基于区块链技术建立的票据交易平台可能会实现上述设想。区块链是一种具有高容错特性的分布式数据库，大量计算机节点维护同一个区块链，通过复杂的校验机制，区块链数据能够保持连续性和一致性，即使部分计算机作假也无法改变区块链的完整性。因此，应用了区块链技术的点对点票据交易能彻底解决许多违法违规的问题。一张票据在申请—发行—交易—承兑整个流程的关键信息，都会记录在区块链上，无法篡改数据，监管部门的查询也是一目了然，更重要的是，其加密数字货币的转移路径明确，为票据交易的可追溯性创造了条件，随着票据业务的不断发展，基于区块链技术开发票据业务平台正在从设想走向现实。

1. 互联网金融背景下的票据业务

2000年以来，票据发行及交易市场呈现较快增长，增幅远超同期其他基础经济指标。在信贷规模严格管控的外部监管和银行内部管理模式下，票据已成为信贷规模紧张和约束条件下的调节工具。如图3-6所示，2010年以来，年末票据贴现余额和承兑余额量逐步增加，贴现余额与承兑余额的比值在近两年大幅提升，2015年已攀升至44.66%。

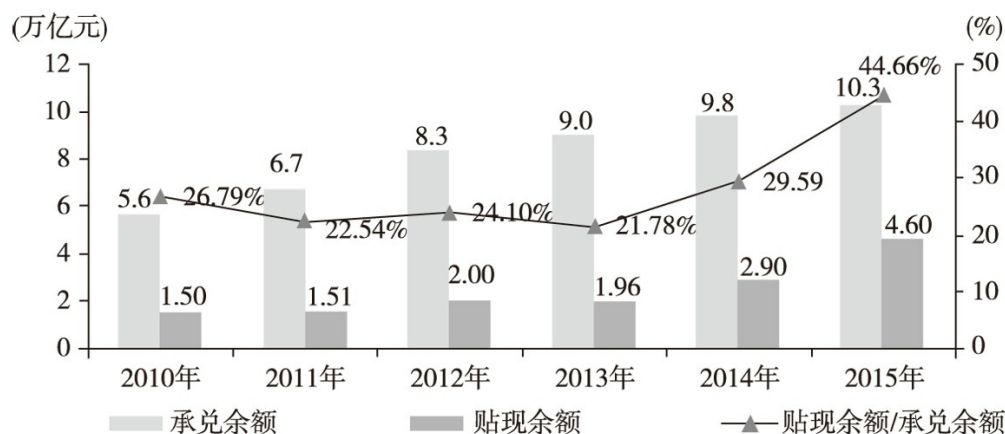


图3-6 2010~2015年贴现与承兑余额

从承兑业务和贴现业务的发展来看，由于受到经济下行压力和实体经济有效资金需求不足的影响，票据承兑业务告别前期的快速增长态势，转而进入相对稳定和平缓的发展阶段；而伴随着票据业务资金化运作趋势的不断增强以及票据资产吸引力的不断提升，各金融机构不断加快票据贴现后的转贴现周转运作，从而使得2015年票据累计贴现量呈现出爆发式增长。2015年，面对传统票据业务模式经营利差不断收窄的现实情况，各类经营机构除采取以量补价等方式外积极探索票据业务创新，同时，市场各类型机构纷纷涉足票据市场和票据业务链条，票据业务创新呈现新的特点。

一是大型银行不断重视买入返售票据业务发展，通过拓展资金业务来提升收益水平，2015年上半年国有银行买入返售票据余额同比增加57.22%；二是电子票据业务得到迅猛发展，2015年前三季度，电子商业汇票系统累计承兑3.99万亿元，累计贴现15.78万亿元，电子票据在票据整体承兑和贴现业务中的比重均超过20%；三是票据理财、票据资产管理等跨市场业务成为机构新兴的盈利增长点，2015年上半年，16家上市银行买入返售票据余额合计2.96万亿元，同比小幅减小，部分商业银行票据资管等业务对原有的买入返售业务产生较为明显的替代效应；四是各类互联网平台层出不穷，民间机构涉足票据业务呈现爆发态势，2015年各类电商平台、中介机构等纷纷成立互联网票据理财平台或信息资讯平台，并通过互联网技术应用拓展移动端票据信息撮合等业务，在整体资金利率下行的趋势下，各类互联网票据平台数量显著增加。

市面上大多数票据理财产品都具有灵活性强、门槛低、期限短、收益较高的特点，因此受到投资者的青睐。截至2016年2月，目前有80家网络借贷平台涉及票据业务，仍以银行承兑汇票为主，累计规模已达到180亿~200亿元。其中京东票据作为京东理财板块下的重点业务，累计交易额接近84亿元，领跑票据市场。目前京东小银票票据产品年化利率为4.30%。

目前市场上的业务模式主要分为票据贴现模式、票据质押模式、委托贸易付款模式及内保外贷模式，其中，票据贴现模式为市场上多数平台的选择。严格意义上来讲，票据贴现是票据质押的一种方式，但其实质相当于票据的直接贴现，平台从中赚取贴现利差，主要以民生易贷-

E票通、小企业e家、票据宝、金银猫等为代表。以金银猫为例，业务流程中，借款人将银行承兑汇票质押给平台，为规避法律风险，票据一般由第三方支付公司或银行托管，随后平台发布借款标的，投资人进行投标。此模式下，借款期限一般与票据到期时间一致，借款人不再赎回票据，借款标的到期后，由平台或第三方托管机构直接到开票行承兑汇票，用承兑金额完成对投资人还款。此外，票据质押模式本质与一般网络借贷质押融资业务相同，但其借款利率较高，还有极少部分平台采用委托贸易付款模式或内保外贷模式，但风险较大。

2. 基于区块链技术的票据业务平台

总部位于旧金山的初创公司BTCJam是全球第一个通过比特币完成网络借贷的平台。在BTCJam平台上，借方只需要创建一个贷款列表，放款人可以直接选择借钱给谁，甚至还可以设立自动程序，只要符合要求的，程序就会自动完成贷款。当然，该平台只能使用比特币交易。当贷款完成后，借方需要周期性还款。BTCJam也会根据用户的表现进行信用评分。该公司的首席执行官Celso Pitta（瑟所·皮塔）表示，绕过法定货币的限制，允许全球的任何人通过其平台接收贷款。BTCJam已经为来自超过100个不同国家的人们募集超过500万美元的贷款。

对于放款人，BTCJam整个应用免费；而对于借款人，低于5BTC的贷款就要收取4%的费用，而其他额度的贷款则只需1%的费用。对于拖延还款5天以上的，也要收取拖延费，这个额度如未达还款金额的5%，最低收取15美元的比特币。

此外，杭州复杂美区块链研究中心已经初步开发完成了一个基于以太坊的区块链网络借贷票据交易所开源项目。复杂美区块链研究中心自2013年开始研究区块链，两年多来整合了金融、餐饮、企业管理、快递追踪等多个细分领域运用区块链技术的理念。复杂美区块链研究中心研发的关于区块链网络借贷票据交易所开源项目如图3-7所示，应用了区块链技术的网络借贷交易所，可以完成无手续费的、每秒15万笔的线上交易。

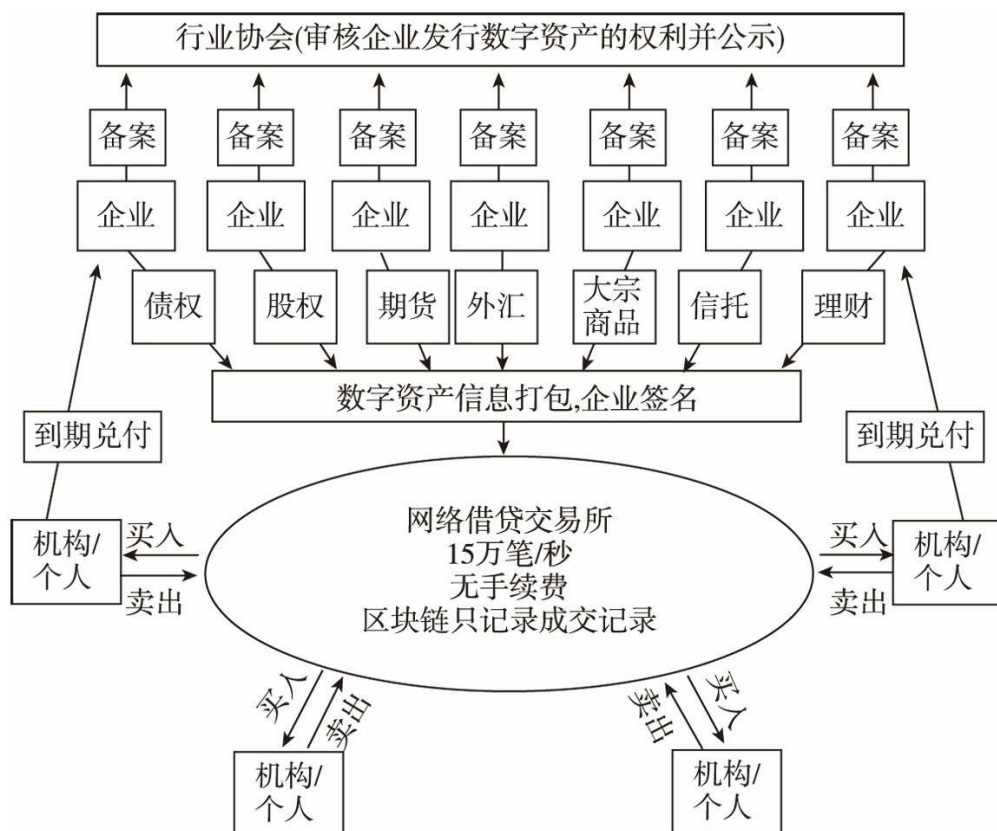


图3-7 复杂美区块链研究中心基于以太坊的区块链网络借贷票据交易开源项目

基于区块链的票据业务将在如下四个方面具有优势：

第一，从道德风险来看，纸票中“一票多卖”、电子票据中打款背书不同步的现象时有发生，但区块链由于具有不可篡改的时间戳和全网公开的特性，无论纸票还是电票，一旦交易，将不会存在赖账现象。

第二，从操作风险看，由于电子票据系统是中心化运行，一旦中心服务器出现问题，则对整个市场产生灾难性的后果，同时企业网银的接入将会把风险更多地转嫁到银行自身的网络安全问题上，整个风险的链条会越拉越长，而借助区块链中的分布式高容错性和非对称加密算法，人为操作产生的风险将几乎为零。

第三，从信用风险来看，借助区块链的数据可以实现对所有参与者信用的搜集和评估，并可进行实时控制。

第四，从市场风险来看，中介市场大量的资产错配不仅导致了自身损失，还捆绑了银行的利益，借助区块链的可编程性不仅可以有效控制参与者资产端和负债端的平衡，更可借助数据透明的特性催促整个市场交易价格对资金需求反应的真实性，进而形成更真实的价格指数，有利于控制市场风险。

金融基础设施革命

区块链对审计行业的颠覆

2011年，微博上一则“普华永道美女硕士过劳死”的帖子引起了网友的广大关注，原来是一名入职审计行业仅半年的员工由于过度劳累引发急性脑膜炎。以上事件虽然属于极端事件，但也反映了审计行业的辛苦以及审计人员从事的琐碎细节工作之多。审计员在进行年度审计和专项审计时，要进行很多必需的专业审计过程来确保所审企业的资金流动、交易往来真实以出具对企业财务报表的审计意见，而这其中的很多过程都是需要大量人力、物力去核实交易的真实性。基于区块链技术的应用能为这些真实性审核提供支持，如果企业间以及企业与银行间的资金往来、交易往来都能够真实无误、不可篡改且有时间戳地记录在全网上，审计员的基础工作将极大地减轻，同时更保证了审计的独立性。所以说，区块链技术与审计行业的结合势必会革命性地改变审计行业。

1. 区块链技术变革审计行业

信任是经济活动的基础，但维持客户的信任不仅昂贵并且耗时，在诸多情况下，效率也不高。在当今的全球经济中，信任是稀有的，这种信任的缺乏，要投入大量资源来进行审计和记录核查，从而降低了经济效率和投资回报率。大量金融服务行业或中介机构的发展都是为了维护金融业的信任，比如银行、托管机构、审计行业等。之所以需要专设机关按照法律对各级政府及金融机构、企业事业组织的财务收支、经济活动进行独立性监督审计，就是因为金融行业或者说经济活动中对信任要求很高，需要专业人员对被审单位进行经济活动监督。而区块链可以被理解为一个基于计算机程序的公开总账，它可以记录在区块链上发生的所有交易。区块链上每个节点都可将其记录的数据更新至网络，每个参与维护的节点都能通过复制获得一份完整数据库的拷贝，这就构成了一个去中心化的分布式数据库。在这样一个分布式数据库里，区块链是利用纯数学方法来建立各方的信任关系，完全不需要第三方，这样建立信任关系的成本也就几乎降到了零。所以目前还未完全发展成熟的区块链技术首先要切入的地方就是对信任要求高且传统信任机制成本高的领域，比如说审计行业。

完成审计业务需要两把尺度：一个是会计准则；另一个是独立审计准则。安然事件中审计失败的主要原因主要就是注册会计师违反独立性，从理论上说，注册会计师与经理人之间不能存在利益上的依赖或管理关系。而问题的症结就在于此，一家企业选择注册会计师的决策权由管理层掌握，注册会计师的选择、聘请费用的多少以及费用的支付方式都可能对被审企业与注册会

计师之间的利益关联形成影响。那么，如何在独立性和有偿服务之间形成有效隔离，区块链技术能够在基础技术层面提供一种可行的解决方案。

利用区块链技术，所有参与人任何数据的更新都会被同步至整个区块链上，而区块链网络上的任何节点都可以查询整个区块链上的数据记录。这帮助审计师在审计工作中对被审单位货币资金交易活动的审核、与其他企业交易往来业务合同及费用真实性的审核创造了条件，也分散了审计结论对于数据真实性依赖的风险。区块链的可靠性保证了经济活动交易记录的准确性，区块链的透明性则大大解决了审计工作中需要大量人力物力去搜集审计证据的问题，也大大降低了审计行业相应的成本。在如今的审计工作中，审计师通常需要发送银行询证函及企业询证函去函证被审单位银行账户资金余额及交易合同或资金的真实性，在区块链技术的帮助下，所有数据都真实可靠透明又不可更改地记录在数据库中，不仅大大节省了函证的审计成本，节约了审计时间，更保证了审计的真实性，避免第三方审计服务机构无法保持与被审单位之间的独立性。全球数万用户、事务所和监管机构共识记账，可以追溯、不可更改，且记账都是盖了时间戳的，这样审计成本一下子就下降了。区块链上能够记载全部真实的数据记录也提高了网络数据的可审计性，审计师未来可以实现对网络中数据的全范围审计。

目前，提供专业审计服务的四大会计师事务所都已明确进军区块链行业。其中，德勤应该可以说是最积极投身区块链技术领域的。该公司透露正在尝试将区块链技术应用到客户端的自动审核以及以众包（公司以自由形式外包给非特定大众网络）的形式开展咨询服务。

2. 德勤和普华永道的共同选择：投身区块链实践

德勤在经过约一年的研发之后，推出了“一站式区块链软件平台”Rubix。Rubix可以说是德勤数字化咨询服务的先锋，该平台应用了区块链最前沿的技术和适用模型，并允许客户基于区块链的基础设施创建各种应用。德勤在Rubix平台上设计一些服务于客户或提升自身企业业务的应用，其中就包括Deloitte's Perma Rec区块链应用技术。这是一个全球性的分布式账簿，通过与SAP和Oracle等各种财务报告系统对接，提高了购销过程的透明度。实时访问相关不可篡改又具有时间戳的数据能够帮助审计师在审计客户公司业务交易往来以及资金交易往来等业务的真实性，以及税务申报等业务是否合规，利用相关数据的实时访问，避免了由第三方审计人员进行审计可能存在的道德风险，使用户与监管部门同时受益。

公司内部会专注于通过开发相应产品解决审计处理中存在的问题。因为公司的每笔交易都在区块链上进行，所以利用区块链设计出的解决方案将会加快审计进度。同时由于区块链具有不可逆性和时间戳功能，对于需要审核的公司，审计师会核查该公司的区块链及全部交易。这将大大加快审计进程，使其更便宜、更透明。德勤亚太区投资管理行业合伙人秦谊女士表示：“区块链技术解决了审计行业在满足公众要求、满足监管部门要求方面的难点，能够保证所有财政数据的完整性、永久性和不可更改性，帮助审计师实现了实时审计，大大提高了审计效

率。”

德勤Rubix平台的业务开发经理和联合创始人Iliana Oris Valiente（依莲娜·奥潘斯·瓦琳特）表示，德勤公司现在有能力构建区块链技术帮助企业客户，她认为这是认识到未来可能性的开端。也许最值得注意的是，Rubix除了为它的客户提供访问多个分布式共识平台的权限，此外还具有利用区块链技术大大提高工作效率、保证财政数据完整性等优势。德勤公司也希望能够掌握最前沿的区块链技术，成为金融行业运用的领导者，能够在客户发现区块链技术的重要性之时，已经可以为客户解决咨询服务。德勤首席资讯官艾瑞克·皮希尼在接受采访时表示，德勤一直就区块链技术潜在的商机进行研究。他表示：“在咨询方面，我认为我们将会见证生态系统从适应、改变到将区块链作为解决方案的过程。德勤的潜力在于通过点对点的众包平台提供大范围的咨询服务，而不是帮助客户制定发展策略。顾客可以在区块链上进行咨询，然后区块链将针对不同的问题匹配合适的公司来进行解决。”皮希尼还补充表示鉴于咨询逐渐成为德勤业务的重要组成部分，公司对于这方面的发展过程也是“非常认真”的。

除德勤以外，在2015年收获了财富100强中43%审计费用的普华永道也已经宣布进军区块链技术行业。2016年1月29日，普华永道与比特币公司Blockstream达成战略合作关系，以帮助企业评估加密货币和区块链技术，并为比特币协议推出新应用。此后，普华永道又与DAH公司达成合作伙伴关系，以获得DAH公司关于区块链技术的支持，从而节约时间成本；不久，普华永道成立了区块链顾问团队，有报道称英国主要金融监管机构的一名前监管者已经被普华永道聘请加入区块链顾问团队。普华永道的转型与创新负责人迈克尔·伦德尔曾公开表示，普华永道预计客户群对区块链技术应用的需求必然会越来越多，公司会积极探索。由此我们不难发现，区块链技术给审计行业带来的变革优势不言而喻，时间成本、人力物力成本、工作效率都能得到较大节省和提高，除审计工作以外，区块链技术对于其他行业的影响也是四大会计师事务所所密切关注的，各家都在努力投身区块链技术的研究，希望能够为客户提供世界级的相关服务。

区块链技术带给审计、金融行业的发展变革值得我们拭目以待。

资产确权——区块链让难题变得如此简单

哥伦布被称为是第一个发现美洲新大陆的欧洲人，历史予以了记载；阿波罗是首次登陆月球的宇宙飞船，也被称为踏出了“人类历史上的一大步”，留在了历史的记忆中。但是在浩瀚的大宇宙中，微不足道的小事与我们息息相关，却又转瞬即逝，正是这些扯不清理还乱的小事，给我们的生活和工作带来了诸多的烦恼。还记得新闻报道上多次有关音乐版权、家族财产的纠纷案件吗？也许，不远的将来，这样的事情就可以得到解决。当你创作的歌曲家喻户晓时，有渠道可以向世界宣告，你是它的第一创作者，所有的网民为你站台；当你急需把手中的股份转

让时，你也不必拿出遗嘱，所有的人都能为你背书。结束这些纠纷的就是区块链技术的应用。区块链技术就像是公正的法官，它会给你最公正的裁判，也像是一把量度的尺子，它会告诉你不可逾越的分界线。

1. 确权的难度

确权是依照法律、政策的规定，经过向有关部门申报、权属调查、审核批准、登记注册、发放证书等登记规定程序，确认某一物体的所有权、使用权的隶属关系和他项权利。在涉及资产的各个领域，无论是房产、汽车等实物资产，还是健康、名誉等无形资产，确权都是交易、追踪的基础，现实中都需要借助第三方权威机构按照法律相关规定予以明确。

从资产的登记、转让、确权以及质/抵押效率的角度分析，无形资产要比有形资产更为困难。主要体现在三个方面：一是评估登记管理不完善，需要较长的时间。在我国无形资产如专利权和著作权做质押登记时，至少要等一个半月，其中公示要10个工作日，等候1周，办理质押登记要再等15个工作日；二是无形资产评估困难，无形资产评估需要专业的评估机构，但是普遍缺少市场认可度；三是无形资产流转处置困难，由于无形资产具有较强的专业性，其价值认定也较为困难，变现渠道较为有限。

2. Factom（公证通）的实践

比特币系统是一个利用动态多重签名DMMS技术支持单一原生数字资产传输的区块链，在比特币生态系统中，比特币的创世和分配通过交易进行，每个人都可以每条交易进行验证，另外每笔有效交易的输入都可以被验证，实现价值的转移是系统的核心功能。基于区块链技术的应用方案的设计核心实际上是在可扩展性和去中心化之间的取舍，可扩展性代表了服务内容的延伸，而去中心化则代表了服务系统功能的安全性。许多不同的团队正在设法基于区块链技术实现超越比特币价值转移的功能。举个例子，交易可以管理域名注册、管理日志安全摄像机镜头、追踪艺术品的出处，甚至还能建立历史数据来显示马匹的价值。

Factom在此方面的创新走在了行业的前沿，并已开发出第一个可供政府、金融等相关机构用于数据保存的区块链应用。通过在区块链上增加一个数据层协议，Factom实现了一个安全且不可逆的数据保存机制，仅仅需要一个哈希就可以安全可靠地保存百万级别的实时数据。Factom找到的方法使得每一条链都可以在不用和其他无关键的信息交互的前提下进行验证，这样就可以最小化信息内容。Factom在区块产生的时间内，记录链上已有的条目，而每一条链都是独立的，通过扫描这些记录，应用程序能够在链上挑出它们需要的内容，Factom的用户只需在他们感兴趣的链上保持验证。

Factom团队的首席执行官彼得·柯比（Peter Kirby）指出，“比特币每10分钟产出一个块，每个比特币块能记录的数据是有限的，这也意味着比特币不能直接用于涉及大量数据的应用。通

过Factom，用户可以对文件进行哈希，并把这个哈希公开发布，这就像为文件制作了一枚电子指纹一样，通过这个电子指纹就可以对文件进行验证。每个数据会被拷贝上千份并分布在世界各地内，同时Factom系统会通过把哈希值上传到比特币的区块链中为所有数据发布一个分布式的哈希表，以此来证明数据的存在，当然任何人都可以通过维护一个节点来更新Factom系统里的数据。”

Factom开发团队已经发布了一个beta版本的系统Factom Genesis，并利用这个系统保存了人权宣言（The Universal Declaration of Human Rights）的443个翻译文本。Factom开发团队还发布了一个Factom公钥生成器（Keymaker），生成器包括3个版本，分别支持Mac、Linux、Windows三种操作系统。

早在2015年7月，Factom公司就通过众筹服务平台Bnk To The Future出售了部分股权，并获得了110万美元的融资。此外，该公司还于2015年7月出售factoids（Factom网络代币）获得了2278比特币（约合54万美元）。2015年10月，Kuala Innovations公司（注册于英国根西岛），以每股1美元的价格购买了Factom公司3.64%的股份，共计40万美元。根据Kuala公司发表的声明，Factom公司的估值目前为1100万美元。

Factom实现这个估值有相当一部分原因来自于已经走出实验室，迈出实际应用的第一步。2015年5月路透社报道称，Factom和洪都拉斯政府建立了合作关系，该国将使用分布式账本技术来记录土地所有权。（洪都拉斯约800万人口，拥有着世界上最高的谋杀率。根据世界银行的数据显示，该国在2013年的人均国内生产总值约为1577美元，这使得它成了西半球最为贫穷的国家之一。在过去，洪都拉斯一直在与土地所有权欺诈做斗争。）根据这个消息，洪都拉斯将是继马恩岛之后，第二个利用区块链技术的政府。Factom的彼得·柯比说，“这个国家的数据库基本上已经被黑了，因此官僚主义者们可以随意在海滨取得自己的房地产。”于是，通过区块链来构建一个不可变的产权记录，洪都拉斯可以越过发达国家建立一个新的体系，预计该试点项目将在2015年底完成。但是之后不久，Factom的创始人Paul Snow表示，Factom未能完成之前所述与洪都拉斯政府的交易，并发表公告称其先前宣布的概念证明项目已经“停滞”，其阻力来自“政治”等因素，但Factom的方案显然为土地确权提供了一个可能的技术和新的思路。

Factom也将中国列为其应用实践的重要领域。按照彼得·柯比的说法，随着全球城市和地区的迅速扩展，预计将会有越来越多的国家和企业拥护技术创新来处理他们的大型数据库和扩张计划。在此，区块链解决方案可以提供更高水平的透明度和问责制，同时降低成本和费用。彼得·柯比在采访中说，Factom模式的美在于它能够通过区块链后台整合所有系统，允许对数据进行永久不变的审计追踪。通过这种方式，就可以建立一种崭新的能够进行问责的方法和防篡改的数据存储库，然而到目前为止，这种类型的存储库还都很容易被任意数量的第三方利益团体所篡改。

2016年2月16日，Factom与杭州安存正信科技有限公司联合发布合作备忘录，双方就Factom公司的区块链技术与安存正信的电子数据证明服务进行融合达成合作意向。安存正信隶属于杭州安存网络科技有限公司，将在业务合作中负责服务和产品的开放型平台的搭建、技术开发和技术维护等。杭州安存网络科技有限公司作为中国电子数据证明与互联网建设的倡导者，与全国100多个地区的公证处建立对接，已研发八个产品体系，包括语音、邮件、凭证、合同、版权、电子政务、医疗数据、即时通信，广泛应用于各行各业。Factom公司将为安存正信提供区块链系统的接口，作为其公证服务后台运行的一部分，并通过双方业务系统的对接，在中国28个省市100多个地区推广使用。

从世界其他国家的发展来看，运用区块链技术的信息系统将有助于智慧城市设施的安全建设，并将提高建设过程的透明度，在明确主体责任的同时节省成本。2016年2月1日，软通动力信息技术（集团）有限公司与Factom联合发布合作备忘录，双方就软通动力的智慧城市解决方案与Factom的区块链技术进行融合达成合作意向。Factom将提供商业和技术支持，协助软通动力利用区块链技术进一步拓展公司业务。作为软通动力智慧城市解决方案的一部分，Factom公司的Apollo产品将提供数据存储、审计和验证服务，在中国数个地区推广使用。彼得·柯比说，“中国最近的合资企业对Factom公司来说是一个很大的机遇，Factom能够展示另一种拓展区块链的方法——将数据层放到区块链上来。双方通过合作最终要解决的问题是避免一定利益相关者对智慧城市的传感器数据造成可能的混淆，基于这个解决方案我们可以设想任何人都不能为他们或他们的企业对城市造成的污染撒谎。”

智能合约——不可思议的区块链技术

传统合约是指双方或者多方通过协议来进行等值交换，双方或者多方必须信任彼此，能履行交易，而智能合约则无须彼此信任，因为智能合约不仅是由代码进行定义，也会由代码强制执行，完全自动且无法干预。密码学家和数字货币研究者尼克·萨博早在1994年就提出了“智能合约”的概念，几乎与互联网的概念同时出现。从本质上讲，这些自动合约的工作原理类似计算机程序的if-then语句，智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。而在20世纪90年代，萨博关于智能合约如何工作的理论并不能实现，主要是因为当时没有能够支持可编程交易的数字金融系统。因此，萨博当时的智能合约理念还只能停留在理论阶段，无法应用到现实中。而随着区块链技术的突破，智能合约获得了重生的机会，让以往人们幻想中“可编程的钱”能够有机会付诸实践。

1. 区块链技术为智能合约带来重生

简单地说，合约的核心层面就是一个要约、一个承诺以及一种价值交换的行为。而智能合

约指的是一种资产的数字化协议，协议的内容包括了标的资产在哪里以及何时将如何执行，这些都是完全基于网络环境实现的，无须托管人干预。萨博将智能合约的定义总结为：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”数字形式意味着合约体现的权利与义务关系可以写入计算机可读的代码中，只要参与双方达成关于智能合约建立的权利和义务的协议，计算机或者计算机网络就可以执行完成。智能合约应用于金融交易具有明显的天然优势，因为金融交易的本质就是价值的转移，在金融交易中被交易资产的本质决定了交易双方选择协议的类型。萨博在1997年的智能合约论文中提到了合约的规范化。他认为多种类型的合同条款，如抵押品、债券、产权界定等，都可以嵌入执行条款的硬件和软件中，通过这样的方式使那些不遵守协议者逃避违约成本的概率降为零。因为，如果当交易双方中有一方没有按照双方协议的合约条款来执行，那么就不会触发合约自动执行，从而使得遵循协议一方的权益得到保护。萨博还提出了非常著名的“自动贩卖机”理论，简而言之就是自动贩卖机利用的是搬运合约，即任何持有硬币的人可以与供应商交易。锁箱和其他安全机制保护储存的硬币和货物不会被破坏，足以允许自动售货机有利可图地在各种各样的区域部署。而类似自动贩卖机，智能合约是通过数字的方法来控制有价值的、各种类型的资产，实现资产控制的不是弹簧之类的安全装置，而是嵌套于计算机可识别的机器语言的基本规则，这种基于数字的执行装置不仅使智能合约可以实现动态的、主动运作的资产交易，而且可以提供更好的观察和核查点。

当萨博在近20年以前提出智能合约理论时，实践一直严重落后于理论，一直没有如何将这个理念转变成现实的清晰路径。现在，技术已经赶上萨博富有远见的头脑，智能合约开始变得可行。其中，最主要的变化就是萨博在智能合约定义中建立的协议，已经被进一步开发，它们以区块链协议的形式出现了。

而像比特币这样的密码学货币正是帮助智能合约成为现实的途径之一。智能合约可以称作是密码学世界真正的“杀手级”应用，很多人都相信在加密货币领域是不需要人类干预就能够自动执行合约，这些合约经过互相协调，成为自动化的资产、过程以及系统的组合。因为比特币本身就是一个计算机程序，智能合约能够与它进行交互，就像它能与其他程序进行交互一样。区块链和其去中心化共识系统的窍门在于保证了每个人都有账本的副本，并使每个人的账本都对最终的协议执行发挥影响。如果每个人拥有的账本副本是相同的，那么人们就无须中心化的机构去记录交易。而智能合约是由事件驱动的、具有状态的、运行在一个复制且可分享的账本之上，并且能够保管账本上资产的程序。对于这样可复制、共享的账本，无须双方向对方证明自己是诚实的。

而当我们利用运行计算机代码开展智能合约时，当双方在商定合约后，互相同意一份代码版的合约，对合约使用的外部数据信息源、如何解决纠纷达成共识。双方在签署智能合约之前，需仔细检查代码，确信不存在恶意漏洞，进行测试并查看试运行结果后再进行签字并部署到账本上。如此运行下来，双方都无须花费时间精力重新核实合约条款，双方都确信合约代码

能够同时满足各自目的。因为它是运行在可复制、可共享的账本上，双方都能够确信程序的输出结果对双方一致。

2. 智能合约：以法律的力量延伸金融服务

如今的一些技术已经可以被认为是智能合约实践的尝试，比如数字现金协议，能够帮助实现网上支付，同时又保留了纸币现金不可伪造性、私密性和可分性的特点。当我们再深入观察数字现金协议，把其放在智能合约设计的更大范围里，我们不难发现这些协议还能被实施到种类繁多的电子无记名有价证券中，而不只是数字现金。如果将它们应用到一个完全的顾客—供应商交易体系里，我们需要的不只是数字现金协议，更需要一个协议能够完全保证交易。如果交易方付款，商品就会被发送；或者商品寄出去，发货方就会收到钱。而智能合约具有大大减少商业交易欺诈事件并降低执法成本的潜力。另一个将会考虑使用智能合约的领域是合成型资产，这些新型的证券由资产证券与衍生品以各种各样的方式混合而成。通过对这些复杂的期限结构进行计算化分析，以往非常复杂的期限结构支付现在可以建成标准化的合约，以低成本进行交易。

与所有的金融前沿技术类似，我们还要考虑如何将智能合约与我们目前的法律系统相协调。智能合约中的“合约”二字似乎难免让人感觉其与法律概念中的合约有某种联系。不可否认的是，智能合约必须被归类为与法律相关的行为，因为我们生活在一个被法律管理和控制的世界，所有可能的经济交易也都被法律管理和控制着。智能合约可以看作是法律系统的进化，而不是消除。有了智能合约，或许很多个人合约的法律核定会在参与智能合约的各方签署之前就确定好，如果有一方未能达成双方协议中的条款，智能合约不会被触发，也就不会自动生效，避免有交易方篡改交易合约、进行违规操作而需其他交易方利用法律手段维权。律师的职责可以运用在竞争市场中生产智能合约的模板上，帮助合约交易方制定合约确保交易质量以及条款的易用性等。此外，智能合约也有潜力为没有优势的人打开接触司法系统的大门。当合约中的某一交易方违约时，另一方若要寻求法律维权是需要花费金钱和时间的，但能够自动执行协议的智能合约却能够帮助那些无法支付法律费用的人们使用司法系统。

此外理论上，智能合约还能在金融方面为低收入者带来福音，能够使得金融机构更乐意接受低收入者带来的风险。在没有智能合约的情况下，如银行等金融机构为了控制风险很少会贷款给低收入者。但有了智能合约，如果贷款者不能按时还款，收回资产对于银行等金融机构而言就变得更为轻松，也就帮助低收入者得到了更多获得信用贷款的机会。

3. 智能合约：更多的应用场景

智能合约的潜能不只是简单的转移资金，我们生活中很多日常用品都能够被连接到物联网上通过智能合约的形式被使用，比如汽车或是房屋门锁等。由于密码学货币的出现，智能合约这一技术正越来越走进我们的现实生活。它可以在我们生活中的很多小事中得到体现。以欧洲

杯比赛为例，假如你赌西班牙队赢，下注500元或者一个比特币，你的朋友赌法国队赢，下同样的注。第一步，你和你的朋友将比特币发送到一个由智能合约控制的中立账户。当比赛结束时，智能合约通过ESPN、路透社或者其他媒体确认西班牙队战胜了法国队，智能合约将自动将你的赌金和从朋友那赢得的钱，发送到你的账户。

再比如已经渗透到我们生活中的打车软件。在实际生活中，Uber或者滴滴等应用程序可以让用户，也就是乘客和司机两端去共同创建智能合约。这些应用程序提供了价值交换的平台，即付费乘车。具体来说，这些应用程序让消费者创建一个包括乘车距离需求、价格以及享受到服务后自动进行付款承诺的要约，而司机可以接受这个要约并提供乘车服务。在这个过程中，双方分别提供了自己所能提供的价值，司机提供了时间和车辆，乘客提供了费用。合约进展顺利的情况下，乘客在特定地点上车并在目的地下车，司机获得乘客提交的费用。

但目前的打车软件合约更像是半自动合约，在这个过程中的某些方面还是需要人类的互动。目前又有一个新玩家Arcade City公司来到了拼车竞技场，这家野心勃勃的初创公司计划使用崭新的方式攻下拼车产业。与Uber中心化管理的方式不同，他们的撒手锏就是去中心化，公司最近正将以太坊整合到他们的运营体系中。Arcade City公司创始人克里斯托弗·大卫独创性地使用比特币众筹获得了一个“免费的Uber公司”。公司的目标是让Arcade City成为第一个大型“主流”的以太坊公司，这就需要调整以太坊来适应公司的非技术用户群，也就是客户和司机，使他们将在世界各地参与点对点交易。Arcade City正在以太坊建立拼车公司模型，首先要从身份和信誉系统开始，建立一个基于以太坊的信誉系统可行性概念验证，用于管理乘客信誉的许多规定将会被编码成智能合约。当然，在测试过程中如果出现各种问题，还会对相关的智能合约进行修改。Arcade City公司希望通过开放的证据、充足的方式来交流和吸取经验，在经过一系列测试完善过程后，还会努力扩大信誉系统，不再只是考虑拼车公司的具体结构，还要转向信誉系统及其他行业系统的互操作性。如今在Uber等中心化管理的拼车公司的司机每天都在担心旧金山总部会降低司机的利润率、担心总部强制干预点对点交易的时候，就不难看出越来越高的“去中心化”的呼声，智能合约的重要性也就不言而喻。

从打车软件智能合约的应用可以看出日常生活中，区块链在物联网领域有着巨大的应用潜力，这也让智能合约的应用大有可为。物联网是一个设备、车辆、建筑物与其他实体通过嵌入软件、传感器和网络相互连接的世界，小到房屋门锁，大到自动驾驶车都可以成为物联网的一部分。但是现在物联网还存在一些问题，比如汽车系统可能会受到恶意攻击，房屋进入系统安全性有待加强，以及互联网普遍存在的安全性问题。但是区块链却有着解决这些问题的潜力。

IBM和三星最近为ADEPT（自动去中心化点对点遥测技术）提出了一个概念验证，使用区块链数据库建立一个分布式设备网络，由ADEPT来提供安全并低成本的设备连接方式。根据可行性执行报告显示，家用电器如洗碗机，可以通过执行“智能合约”来发布命令，要求洗涤剂供应商进行供货。这些合约给予了设备支付订单的能力，并且还能够接收来自零售商的支付确认

消息和发货消息，并以手机铃声提醒的方式通知物件主人。通过这些都可以看出在物联网的概念中，区块链技术在未来的应用场景不仅仅是在金融等领域，在生活中给我们带来的便捷和改变更是比比皆是。

最后，我们将智能合约的概念延伸到财产上。智能财产的建立可以通过将智能合约嵌入有形的实物里。这些嵌入的协议基于合约条款将运作财产的钥匙控制权自动交到财产的合法代理人手上。例如，一部车为了防止被偷窃，除非确定拥有者完成正确的“挑战响应协议”（challenge-response protocol），否则车是不会启动激活的。如果车是贷款买的，拥有者无法偿还贷款，智能合约将会自动调用扣押令，并将车钥匙的控制权交给银行。这个智能扣押令（smart lien）应该比回购人机制更便宜也更加有效。同样需要的是当贷款被还清的时候协议可证明地移除扣押令，并排除一些运行中的困难情况。

智能合约是通过区块链协议建立的应用之一，目前围绕区块链应用和智能合约已经建立了两种协议：一种是大名鼎鼎的电子加密平台以太坊；另一种是建立在比特币区块链侧链上的Rootstock。

4. 以太坊（Ethereum）智能合约的基础设施

当今非常火爆的以太坊最初是由一名20岁的俄裔加拿大天才科学家Vitalik Buterin开发的，他凭借其在计算机方面无与伦比的天赋，在数字资产行业拥有极高的地位。这位被称为“天才神童”的以太坊创始人出生于1994年，2011年全年为比特币线上媒体《比特币周刊》工作，2011年后作为联合创始人创建了《比特币杂志》，曾击败Facebook创始人扎克伯格，获得2014年IT软件类世界技术奖。智商超高的Vitalik甚至还在很久之前就自学中文，在与中国社区用户交流的活动中多次用流利的中文为区块链爱好者解答各类问题。那么，到底什么是以太坊呢？以太坊是一个平台和编程语言，能够让开发人员建立和发布下一代分布式应用，可以说是为开发者提供了一个创建和发布他们各自区块链应用的平台。以太坊可以用来编程、分散、担保和交易任何事物：投票、域名、金融交易所、众筹、公司管理等，而这些托管应用程序的计算能力是由一个网络来供应的，人们分别贡献自己计算机的处理能力来维护和运行这些应用程序。以太坊平台的多功能性和能够创建、执行智能合约的能力都使它成为银行与金融科技产业的重要选择。通过使用智能合约，金融机构、交易平台甚至银行部门都能够使他们的后台程序自动化运行，减少整个流程所需要的劳动力和时间。使用以太坊技术平台的主要公司包括纳斯达克，银行区块链财团如摩根大通、高盛集团、Visa等。

虽然智能合约的实践发展是基于比特币而产生的，但比特币目前有限的智能合约开发环境也引发了公共区块链的竞争，例如以太坊从理论上来讲就可以运行更复杂的合约。况且公共区块链的交易确认时间，在一般情况下会比私有网络用时更长。但据新的研究表明，比特币的技术也可以克服这些限制，并获取更多的好处。例如，开发人员正在研究被称为机密交易的加密

工具——同态加密，以提高安全性。同态加密是一种无须对加密数据进行提前解密就可以执行计算的方法。该工具可以在无须了解交易输入数量的前提下验证一笔公共区块链的交易，这样就提供了更好的隐私性，也是金融机构最喜欢的特性。这种技术允许用户在解决一笔交易时，无须透露它的金额大小，也不用向他人展示账户金额情况。公共区块链的隐私将通过使用“零知识证明”得到进一步提升，除了声明的有效性，这个验证方法并不会透露其他的信息。使用同态加密技术在区块链上存储数据可以达到一种完美的平衡，而不会对区块链的属性造成任何重大的改变。也就是说，公共区块链仍然是公共区块链，只是区块链上的数据将会被加密，这就解决了公共区块链的隐私问题，同态加密帮助公共区块链达到了私有区块链的隐私效果。而同态加密技术不仅提供了隐私保护，它同样允许随时访问公共区块链上的加密数据进行审计或其他目的。如今这样的项目有Zcash，这是一个在公共区块链上的开源加密货币促进支付系统，但是发送方、接收方以及交易的金额都是保密的。就好比当前能通过网络来构建安全的电子商务交易一样，未来在公共区块链上构建私有业务也是有可能的。公共区块链平台也支持智能合约，所以在一定程度上吸引了一些主要金融机构的关注。

5. 侧链和闪电网络：另外的可能

在以太坊越来越受到世界关注的同时，2015年12月Rootstock横空出世。开发者试图通过“侧链”来解决比特币可扩展性的问题，开辟了新的用于实验的可能性。Rootstock是一个建立在比特币区块链上的智能合约分布式平台，它的目标是将复杂的智能合约实施为一个侧链，通过在比特币的一个侧链上建立一个全功能的“图灵完备”的智能合约平台来为核心比特币网络增加价值和功能，这也就意味着Rootstock不仅是用于双方之间的价值交换，而可以用于更复杂的交易。与以太坊不同的是，Rootstock使用不同的开源区块链协议来建立智能合约，它实现了以太坊虚拟机的改进，开发团队通过使用可转换为比特币的代币作为智能合约的“燃料”而移除了以太坊“ether”这种代币的需求。值得注意的是，尽管Rootstock是建立在比特币侧链上的，但它使用的却是与以太坊操作码相结合的图灵虚拟机。这样Rootstock就完全能够与以太坊平台兼容，在Rootstock区块链（也就是比特币侧链）和以太坊区块链上都可以完美运行。以太坊和比特币两大区块链平台的结合和兼容性使得Rootstock的优势更加明显。据2016年3月22日的消息，区块链创业公司RSK Labs已宣布获得了100万美元种子资金，用来支持Rootstock的发展。

说到智能合约，就不得不提到闪电网络理念。什么是闪电网络呢？它的主要目的是实现安全的链下交易，其本质是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制，通过设置巧妙的“智能合约”，使得用户在闪电网络上安全进行未确认的交易。2015年2月，约瑟夫·朴恩（Joseph Poon）和萨帝厄斯·追亚（Thaddeus Dryja）发布了一篇他们称之为“闪电网络”的草稿。当时它仅仅是一份不完整的建议，并且没有代码，但它引起了比特币技术社区相当大的兴奋，因为这份草稿让大家看到了即时任意方支付比特币的可能性。可以说，闪电网络就是比特币的一个缓存，基本设计是基于一个网络支付渠道。闪电网络的交易就是未确认的比特币交易。闪电网络不会持有任何人的资金，所有的资金都存放在比特币网络中的多重签名资金交易

中，闪电网络所做的就是让参与者之间的签名交易更加方便。简单来说，比如在比特币交易中，双方建立一个交易链，交易链中的交易只有最后一笔需要进入真实的比特币区块链，这就是简单的支付渠道思路。事实证明，只需要少量几乎没有争议的比特币升级，人们就可以生成更加通用的支付通道，它允许双向支付，也允许“条件支付”，条件支付允许构建一个支付网络。实际上，可以通过安全和非信任依赖的方式设定“如果A支付了B，我就支付给C”等智能合约。合约条件发生之后，你的钱包就会自动向比特币网络广播这个支付交易条件，然后只需等待即可。闪电网络这种支付渠道的理念是能够解决比特币可扩展性、小额支付和0确认问题的可行途径，帮助参与者之间直接进行交易，而不是通过区块链发送交易和使用它加密来确保信息安全，只需在最后结算机制时才使用区块链。基于此，闪电网络可以说是链下去中心化交易的杀手级概念应用，当然目前闪电网络还不存在，但如果我们能够在应用实现这种概念，免费、实时地执行数十亿的小额交易，那么闪电网络的确能够解决我们目前的许多问题。

像比特币这样的密码学货币已经准备就绪，足以帮助智能合约成为现实，最终可能会实现密码学货币和智能合约的双赢。智能合约能够向人们说明虚拟货币独特的益处，这将为虚拟货币吸引更多的用户。智能财产可能是一个很长的路，但是数字现金和合成型资产今天已经出现了，更多的智能合约机制正在被设计出来。到目前为止，对来自截然不同领域如经济学和密码学的自动化合约执行来说，设计准则是很重要的，但两者缺少交叉沟通，一边是对技术缺乏意识，另一边对最好的商业用途缺乏意识。智能合约的理念是要认识到为共同目标而做出的努力，这将在智能合约的概念上进行交汇。

第四章

链接万物的区块链

区块链技术在大数据时代有着越来越广泛的应用，除了金融领域，区块链去中心化、不可篡改又具有高透明度的技术特点已被发现能够在多个领域展开应用。如何高效解决互联网虚拟世界的秩序混乱及诚信的建设，其难度已经不亚于证明“我妈就是我妈”这类问题。如何才能以较低的成本提高数据证明过程的透明度；如何通过分布式数据库以更低成本明确权属；如何通过区块链点对点通信的技术提高投票决策的效率；如何利用智能合约赋予物联网更高的安全性、智能性和可扩展性；如何和现有电商业务结合，开启另一个共享经济的时代？这些疑问也都是我们对于区块链技术变革生产生活方式的期待。

这个房子属于我吗——区块链给你证明

区块链是一个公共记录账本，存储于全世界数以千万计的计算机之中。存储信息具有的公开公证的可复制性与不可更改性，使得这种公证比目前各国使用的传统公证方法更安全。区块链技术在法律方面尤其是在法律公证和财产公证方面更能大显身手。比如，一些民事领域时常出现举证定责难的情况，而区块链技术则可以记录下每个步骤，帮助司法机关认定具体责任人。尤其在资产领域，无论是房产、汽车等实物资产，还是健康、名誉等无形资产，都能利用该技术完成登记、交易、追踪。甚至大宗商品的交易，诸如贵金属、期货或证券都可以通过智能编码，将信息写入区块链中来实现。我们通过案例来了解这种应用。

如何继承父母房产

首先，让我们先来看一个真实的案例。

小丽是父母的独生女儿，父亲10年前去世，母亲也刚过世。父母生前留下一套127平方米的房子，大约价值300万元，房产原先登记在父亲名下。父亲去世时小丽还未成家，因此就没去办理什么手续。现在母亲也去世了，而小丽也已经成家，女儿两周岁，再过一年就上幼儿园了。因此小丽就想把房屋过户到自己名下，然后把自己和女儿的户口迁到房子里去。

小丽拿着房产证和父母的死亡证明到了房管局，要求过户。房管局说仅凭这些东西没法给小丽办过户手续。小丽要么提供公证处出具的继承公证书，要么拿法院的判决书，他们才给办。小丽没办法，谁愿意没事打官司啊，就马上去了公证处。“公证处的人说让我把我爸妈的亲戚全部找到，带到公证处去才给办公证。可我爸妈的亲戚全国各地都有，有的都出国了，我到哪去找他们？”小丽找到律师说明情况时，还没说几句就哭了。

据律师介绍，此类事件并非偶然事件。律师已经接待过大量类似的继承疑难复杂案，而且根据律师接待过的经验，根据现有的法律，即使她费尽周折找到她遍布全国甚至在海外的七大姑八大姨，众堂表亲兄弟姐妹，她也不一定能达到将房子过户到她名下的目的。

洪都拉斯的拆迁纠纷

再看一个国外的案例。

一位在洪都拉斯的老太太住在自家房子30多年，某天忽然来了警察要将她赶走，原因是国家财产局的记录显示，该房子为另一人所有。住了30多年的房子竟然属于另一个人？如何证明我的房子就是我的呢？老太太出具了土地凭证，但法院也未予采信，仍然依据国家财产局的记录为准判房屋归属另一人，老太太无奈地眼睁睁看自己住了几十年的房屋被拆毁。而当老太太的家已经被拆毁以后，法院才发现，财产局的记录有误，房子确实是老太太的。

类似这样因为有意无意的记录错误而导致的不公正与财产损失，每天都在世界各地发生。但人们对此无可奈何，因为最终判断的标准掌握在少数人手上。

传统认证系统的缺点

1. 速度慢，无法快速查找、上传、下载相应的数据

在现有的情况下，记录靠手工完成，所记录数据的保护、同步更新和真实性的验证都非常困难。其中的一部分流程在实现了计算机自动化以后，并没有变得容易，反而是更加困难，因为电脑记录很容易被人为更改。

2. 成本高

需要经过多家机构的多次确认，交易成本高。尤其是在我国现有的条件下，很多认证的成本已经高到让交易无法进行的地步。

3. 存储复杂

需要有权机构进行集中物理存放。这种集中物理存放不仅管理复杂，而且存在着较大的风险。一旦统一的电子托管器发生损毁，很多资料就无法恢复。

4. 信任缺乏

在当今的经济条件下，信任是稀有的。这种信任的缺乏，造成了大量的资源投入来进行审计和记录核查，从而降低了效率和投资回报率。

区块链技术可以解决公证和认证的问题

1. 不可复制

每个区块就像记账本，含有不同密码，当中的电子货币是由一组独特密码组成，也可以理解为区块链的唯一性。

2. 去中心化

交易发生时，讯息会发送给所有参与者，由计算机交叉运算认证，而非仰赖权威机构。

3. 不可篡改

认证完成后交易即生效，无法反悔收回，也可以理解为不可篡改性。

4. 透明公开

交易产生的“账本”链接到其他账本上，交易明细都被记录下来，任何人都能查证此笔交易。

所以回到刚才小丽的房产证明纠纷，只需要爸爸写一个房产证明，生成一个PDF文件，并发送到区块链上，生成一段“符号加数字”，我们可以将其理解为一把私钥，并将这段“符号加数字”告之小丽，万一发生了房产纠纷，不需要爸爸或者其他公证机构的认可，我们只需要小丽拿着这段“符号加数字”，系统就会自动识别这段“符号加数字”，如果与当年爸爸留下的“符号加数字”相符合，就证明了小丽的这个房产证明就是当年爸爸留下的那份房产证明，就这么简单。

从Stampery到Chronicled，区块链公证业务的实践

Stampery就是这样一家利用比特币区块链技术代替公证人的创业公司，能为所有的敏感文件提供具有法律约束力的证明。可以用Stampery证明任何文件，它能很好地保护知识产权，证明遗嘱、宣誓、合同、家庭纠纷中的通信等的有效性。你要做的仅仅是通过电子邮件把文件发给你的个人专用Stampery电子邮件地址，用Stampery的网站上传文件，通过API将Stampery整合到你的产品中，或者将Stampery与你的Dropbox关联。

相比文件公证，Stampery的优势在于你不必带着纸质文件亲自去公证人那里，能节省不少时间。对于每月发送少于100个文件、使用储存空间小于1GB的用户，Stampery是免费的。每月付费9.99美元，就能储存多达1万个文件，储存空间能扩展到100GB。

Stampery目前的主要目标客户有三种——需要证明文件的律师、需要证明图片和视频的创作者人以及想保护其知识产权的创业公司，在与政府机构合作时，提供的认证服务便捷而且更安

全。这种无信任系统在这个世界上任何一个地方都可以被独立验证，以及在保护知识产权方面都将有所建树。由于使用了这类认证系统，对于重度依赖公证文件的专业人士来说非常轻松，区块链技术公证优势比传统的公证大得多，虽然现在面向的市场很小，在未来的市场中将会占有很高的份额。

Stampery公司还将推出一款电子邮件标记系统，让用户有证据证明他们发送了某个邮件，同时在区块链上获得这封邮件被收件人打开的证明。如果发件人想让收件人就电子邮件上某些内容发表看法，Stampery可以让该用户在邮件中设置一个“同意”按钮，这样全部收件人对邮件的表态就可以被存储在区块链上。

由于法律证明是储存在区块链上的，任何人都可以检索到这些证明。Stampery与其他电子公证服务的不同之处是，公司没有集中化数据库，这也意味着公司不会被黑客攻击，而每一个证明依然能够被验证。但需要提醒读者的是，由于区块链的概念还很新，目前还没有人在法庭上使用它。

Chronicled是一家利用区块链技术来帮助验证收藏类运动鞋的创业公司，它已获得了由香港风险投资公司曼图资本（Mandra Capital）领投的342万美元种子轮融资。其他投资方包括黑豹资本（Pantera Capital）以及Colbeck资本管理公司。成立于2014年的Chronicled公司旨在使用“智能标签”来确保消费者产品的真实性，它可以插入鞋子并连接到用户的苹果或安卓应用。然后Chronicled会使用区块链技术将鞋子的信息记录在一个分布式账本上。

Chronicled希望该系统能够针对三个目标市场：收藏家，在购买收藏品时能够省心；零售商，想要卖真货；品牌商，它们寻求利用“智能标签”来吸引消费者。据Chronicled公司表示，它将推出运动鞋认证服务。

我还是我吗——在区块链上很简单

在当今社会，有很多时候需要我们去证明自己、证明家人、证明工作、证明房产，等等。去政府机构进行漫长烦琐的手续证明实在让我们头疼不已，不仅如此，有时候甚至让我们不知如何进行证明。难民身份、重婚危险都是身份证明曾经带给我们的困扰，而区块链技术如何改善这一情况呢？

如何证明“我妈是我妈”

“该怎么证明我妈是我妈！”这是北京市民陈先生的一句感慨。听起来有些好笑，却是他的真实遭遇。陈先生一家三口准备出境旅游，需要明确一位亲人为紧急联络人，于是他想到了自己的母亲。可问题来了，需要书面证明他和母亲是母子关系。可陈先生在北京的户口簿只显示自己和妻子、孩子的信息，而父母在江西老家的户口簿上早就没有了陈先生的信息。在陈先生为此感到头大时，有人指了一条明道：到父母户口所在地派出所可以开这个证明。先别说派出所能不能顺利开出这个证明，光想到为这个证明要跑上近千公里，陈先生就头疼恼火：“证明我妈是我妈，怎么就这么不容易？”而更令陈先生窝火的是，这一难题的解决，最终得益于向旅行社交了60元钱，就不需要再去证明他妈就是他妈了。

陈先生的遭遇并非孤例，很多人在办事过程中都遇到过类似的令人啼笑皆非的证明：要证明你爸是你爸、要证明你没犯过罪、要证明你没结过婚、要证明你没有要过孩子、要证明你没买过房……这样那样的证明，有的听起来莫名其妙，办起来更让人东奔西跑还摸不着头脑。而利用区块链技术，比如使用分布式智能身份认证系统，一切信息证明都不可篡改又无误地记录在其中，既不会让私人信息泄露给不法分子，又能在有需要的时候立刻为自己的一切信息做出证明。

如果区块链的技术得到广泛应用，每个人都可以通过家庭关系来证明自己的存在与身份，个人信息被记录在区块链上，就像记在一个分布式公共分类账本上一样。我们如今的身份证就是一个条形码或者二维码，首先它不容易丢失，还有一个好处是万一你不幸成为难民，即便你没有银行账户，也可以凭着这个二维码申请比特币的信用卡，以及接受来自家人、朋友给你的紧急救助资金，而这一切不需要你去任何机构办理任何证明。

分布式智能身份认证系统

不论是Facebook、LinkedIn（领英）还是Twitter这样的网站都会要求用户注册、填写资料、设置交易密码、查询密码等。但注册手续烦琐，而且同时也失去了用户数据的控制权，因为一些私人信息留在网站的信息库里，有可能会被别有所图的“不法之徒”盗取，而用户除了表示不满、气愤之余，没有任何有效的手段。

如果像Facebook这样的网站愿意接受第三方网站提供的用户信息进行注册和登录，那么用户会很乐意使用第三方网站管理个人信息，尤其是这个第三方网站使用去中心化的分布式身份认证系统。

如图4-1，在这样一个智能身份认证系统中，你需要选择一个独有的名字作为其他人能够通过此名字寻找到你的区块链ID的方式。而将此区块链ID与你的其他社交网站相连接验证，就能够确定你的区块链ID所属权并证明你的身份。创建了你独有的区块链ID后，会生成你的在线头像（Online Avatar），将其他社交网站链接到智能身份认证系统中生成联系信息（Contact Information）；同时还会显示你的护照照片（Passport style photo），在姓名下方会有一个密钥创建日期（Key creation Date），这是不可更改的，而你独一无二的密钥标识（Key ID）就在智能身份卡的右上方；在护照照片下会有两个独属于你的二维码，分别链接到你的智能身份认证系统（Keybase.io Link）和链接交易（Transaction Link）的二维码；二维码左边则为子密钥信息（Subkey Information），右侧是签名栏（Signature Box）；身份认证卡的最下方则是交易表示（Transaction ID）以及哈希算法证明（Proof Hash）。

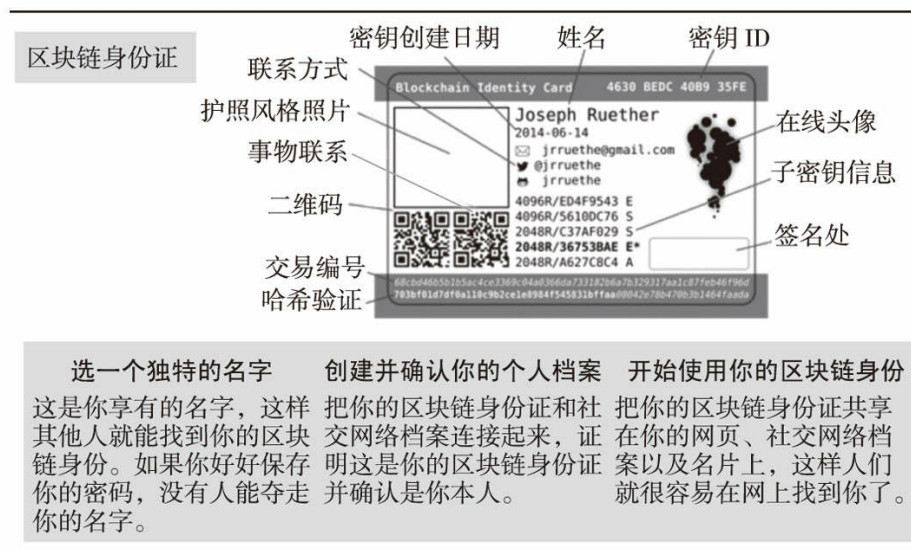


图4-1 智能身份认证系统

资料来源：<http://jrruethe.github.io/blog/2015/03/27/physical-blockchain-identity->

card/

可以把这个智能身份认证系统想象成“一张电子身份证”。里面包含了你的姓名、出生年月、邮箱、联系信息、电子钱包地址、密钥创建日期、护照照片等信息。现在有这样的一套分布式身份认证系统，能让你安全、便捷地解决信息丢失问题。因为这套认证系统可以让你的信息完全掌控在自己手里，永不会丢失，永不会被篡改。

需要提醒的是，你一定要妥善保管密钥，因为无论进行任何操作，都需要提供密钥来进入账户，如果不幸丢失了密钥密码，你的信息将会永久地放在那个“黑匣子”里，因为唯一的密钥只有你自己知道，世界上没有第二个人知道，但你可以对它进行备份。

区块链上享受结婚证明

我们再来分析一个国外的案例。爱沙尼亚的e-居民项目也许是这个星球上最先进的技术之一。作为世界上第一个以区块链为基本元素的虚拟化国家，其提供“DIY管理服务”，除了向难民提供紧急回应和区块链国际身份，该虚拟国家还提供开创性结婚证明、地契、出生证明等。在这个去中心化的管理项目中，无论居民身居何处、工作为何，都可以在区块链上拥有结婚证明和商务合同等等。

这份协议的签订标志着我们向大规模去中心化迈出了更大的一步。区块链技术的出现不仅可以解决当前的难民身份确认难题，也可以享受结婚证明。从本质上我们可以相信这种技术将最终消除国与国之间的国界，从此世界是“平”的。

2015年12月1日，是Edurne和Mayel的好日子。这对夫妻自称为“glomads”，他们经过不断地旅行和探索，决定不再支持任何一个国家或者法律。他们签订了自己的婚姻合同，有效期仅仅只有42个月，并且合同还将保持开放，可以随时更改。这种灵活的协议，在传统的法律框架下是无法完成的，因此他们决定创建一个属于自己的、符合他们预期的婚姻管辖权。在区块链上这种婚姻是可以被证明、被记录、被认可的。再比如说，很多国家规定同性恋非法，但区块链上却没有对性别方面的限制。如果一对新人在公证处结婚，并不是说他们在爱沙尼亚司法系统下结婚，或者在其他国司法系统下登记结婚，而是他们在“区块链司法管辖”下登记结婚。

爱沙尼亚的e-居民项目倡议，可帮助全世界所有人使用安全的、可信的在线网络身份，目前爱沙尼亚政府已经向其130万居民提供了此项服务。爱沙尼亚e-居民项目的项目主管Kaspar Korjus介绍说：“在爱沙尼亚，我们认为每个人都应自由地选择最适合他们的数字、公共服务，而不管他们出生地的差别。我们处于一个伟大的时代，传统国家与虚拟化国家在国际市场上互相竞争、互相合作，为居民提供最好的政府服务。

区块链技术不仅为银行业、公司合同提供了一个具有全球法律约束力的证明，并且以具有完整的合约性、快捷、低成本的技术形式为我们的生活带来了极大的便捷，并同时能更好地维护全球企业家和居民的权益。

DAOs（去中心化自治组织）

在人们做决定的过程中，尤其是涉及做出一些公共决策的时候，投票仍然是解决问题的常见方法之一，它为每个人提供平等的机会。尽管世界各国都会使用电子表决系统，但是仍旧需要花费几个小时来进行人工验证，即使是在美国，投票舞弊也真实存在。2012年，在美国司法部民权分部工作的Justin Levitt（斯汀·列维特）教授表示，在过去12年，投票舞弊概率为0.000002%。而选举的整个过程如果使用分布式账本，就能够有效地将舞弊现象降至更低，因为每一位选民的投票都将被真实地记录在区块链上，不可篡改、真实可信又能实时产生选举结果，无须中心化的人力成本。

即将诞生的区块链总统

2016年1月，有文章发表了关于投票机器的专利应用程序，文中描述了如何使用个人密钥登录投票数据和如何用公开密钥在分布式网络公开结果。签发的投票数据会用公开密钥存储在由投票机器控制的区块链数据中。

目前运用区块链技术选举总统也并不仅是理想中的设想展望，在现实生活中，已经有国家在积极推进实践。根据2015年10月16日CoinDesk的报道，秘鲁的一个政党正在寻求利用区块链技术帮助其进行总统竞选。PerúPosible（秘鲁可行党）是秘鲁前总统阿莱杭德罗·托莱多（Alejandro Toledo）领导的一个政党，其在为2016年4月的总统选举做准备。希尔默·雷耶斯（Hillmer Reyes）是托莱多竞选的政策主任，也是该党的全国委员会成员，他向秘鲁当地一家名为El Comercio的报社透露，该党建议使用区块链技术来缓解社会矛盾、打击腐败现象。雷耶斯向CoinDesk进一步透露了他们的这一计划，概述了他们在选举的准备阶段起草了正式的政策建议，聚焦区块链技术在改善政府服务方面的作用。雷耶斯指出，一些社会问题上的分歧往往造成社会冲突，而区块链技术可以作为一个潜在的解决方案。

2016年2月又有新消息传来，乌克兰也准备使用区块链选举系统，并为此修改了法律。在乌克兰，接下来一系列的选举都可能会使用以太坊区块链。这种电子选举系统即使在全球的投票方式中，也算是相当新奇的。乌克兰采取的区块链选举系统采用了智能合约的模式，而其选择智能合约的一个重要理由就是乌克兰有一组需要特别考虑的监管法规。完成选举投票首先需要注册为投票者，而混合解决方案是不被允许的。一个彩色币有可能代表不同的投票，这将会让所有的选票被宣布为无效。而智能合约能够规避这些问题，其是以太坊区块链原生的或者是发

行的新资产，部署了原生的智能合约，会把乌克兰政治方面的差异性放入到账户中。当系统被调用时，允许进行任何层级的选举，并且提供足够的可扩展性。

2016年4月，美国总统大选也采用了区块链技术，德克萨斯州自由党在三个分开的区块链上大范围地记录选民公投结果，这也是最近把区块链技术融合进投票过程的项目范例。自由党合伙人区块链科技公司（BTC）为此项目创建了Florincoin区块链，250名代表和100名自由选民的投票提名会被记录在Florincoin上，而且可以看见每一个单独的投票。

BitNation（比特国）

BitNation创新性地将区块链技术应用到了公民管理问题，并创设了世界上第一个虚拟的无国界、去中心化的自治国家。BitNation基于以太坊开发了一份包括140行代码的智能合约，通过智能合约这种无国界的技术，BitNation希望消除国与国之间的地理界线，为终端用户提供程序更透明、管理成本更低的去中心管理服务。

BitNation提供了一系列低成本、高效率的公共服务，包括出生证明、结婚证、土地产权证和营业执照的办理；而且BitNation开始为难民提供服务，其中包括保险、基本收入以及其他基于区块链技术的应用。

比特币ATM公司CoinOutlet的创始人兼首席执行官Eric Grill（埃瑞克·戈尔）表示，BitNation对于各个领域的改变是非常巨大的，他希望它能够成为任何一个世界公民的护照。利用BitNation的服务，任何人都能够在区块链上进行验证，而不是去法院和政府机构进行漫长的等待。BitNation使用区块链技术就是很好的实践案例，它引入了一个创新的方法让人们生活的世界变得更简单也更有保障，虽然这个方法还有待长时间的探索与实践。

区块链上的DAOs

BitNation的尝试实际上预示了DAOs（Democratic Autonomous Organizations）这些类组织需要依赖于区块链而存在。从治理的角度来说，社区规则要由所有缔约方共同制定，社区规则的内容可以包括工作分配、资产分配，甚至指定股份的分配。DAOs的两个显著例子就是Slock.it和DigixDAO。

区块链让物联网真正链接万物

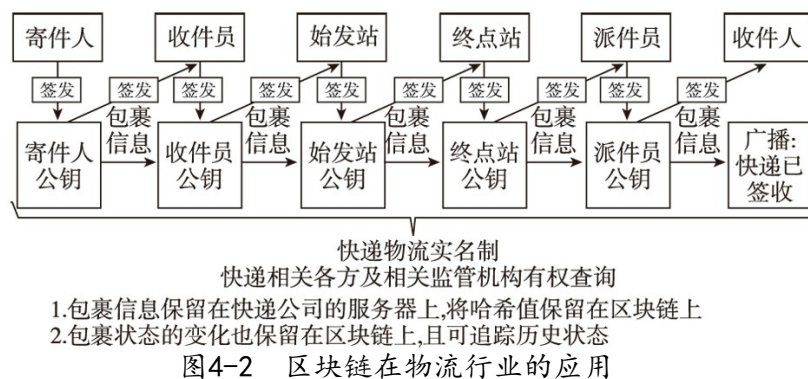
区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了过去10分钟内所有比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块，我们可以把它想象成一个总账本。在这个总账本中，记账员不用去关注一个节点上的数据到底代表欧元、美元或者其他资产，用户也可以自行决定比特币所代表的资产。每个比特币都可以被分割为1亿个最小单位，每个单位都可以单独使用、单独程序化，这意味着用户可以给每一个单位分配属性，用一个单位来表示美元、欧元、人民币、公司股份、一度电、一个快递包裹或者所有权数字证书，因此比特币不仅是钱或者支付方式，比特币可以代表任何财产。

在物联网的时代，运用区块链技术可以直接在机器与机器之间进行经济运行，比如说自动售贩机和无人送货机，这些机器原来无法处理信任的概念，但是借助区块链技术这一切都可以做到，无人机可以准确无误地将包裹递送给收货人，并且确切地知道货款是否已经支付。在去中心化的物联网中，区块链是能够促进交易处理和交互设备之间协作的基础架构。每个区块链管理自己的行为，发挥自身的作用，这样就会形成一个“去中心化的自治物联网”。

更安全的物流和供应链

区块链是一种高度容错式的分布式数据库。2015年11月发表的《区块链项目白皮书》中表明，区块链技术可以记录货物从发出到接收过程中的所有步骤，创建共识网络，能直接找到快递中间环节的问题所在，也能确保信息的可追踪性，从而避免比如“双十一”快递爆仓，丢包、误领、错领等问题的发生，也可有效地促进物流实名制的落实。

利用区块链技术，在快递交接时需要双方私钥签名，每个快递员或快递点都有自己的私钥，是否签收或交付只需要查一下区块链即可，最终用户没有收到快递就没有签收，快递员无法伪造签名，杜绝快递员通过伪造签名来逃避考核，减少用户的投诉。同时，企业也可以通过区块链掌握产品的物流方向，防止窜货或打假，保证线下各级经销商的利益。



资料来源: <http://www.mingjin.com/btc/news/5293-1.html>

2015年5月,在2015创新中国(DEMO CHINA)春季峰会现场海外专场中,来自加州硅谷的Skuchain团队就中国进出口贸易现状与问题给出了自己的看法与分析,并给出相应地解决方案——Skuchain,把商品流和资金流结合在一起使它们同步,并且利用现代密码学技术以及现代数学方法进行整合。

中国现在是进出口大国,自2013年起国际贸易额就超过美国,排名世界第一,但同时也产生诸如假货、伪劣产品等问题。Skuchain公司致力于建设新一代供应链来解决这些问题。2016年3月31日,有微信公众号发布信息称,可瑞康正式宣布退出中国市场,理由只有一个:代理商进口了一吨奶粉,结果卖出了十吨的销量,这说明有9吨奶粉是假奶粉。而发生这一问题的原因是商品流动和资金流动没有同步,Skuchain公司可以运用区块链技术把商品流和资金流结合在一起,使它们同步,这意味着我们将现代密码学技术以及现代数学方法整合后,可以使用二维码,更方便地去了解商品的信息。

Skuchain的工作原理很简单,以进口红酒为例,假设我们有144瓶红酒,分成三部分给了经销商,因为总数是144瓶,所以不会产生145瓶红酒,我们可以做到把其中一瓶红酒或者是几瓶红酒转让给下一个经销商,而经销商不能复制二维码,如果复制的话系统可以跟踪到谁复制了这个二维码,谁企图复制侵犯商品权,制造假货的人就会受到惩罚。Skuchain公司目前的主要客户群来自一些奢侈品品牌和大牌商品,比如说新西兰的牛肉、蜂蜜、龙虾以及红酒供应商。

智能物联网

区块链技术解决了物联网的核心环节,IBM早在2014年就开始着手研究区块链;近期国内万向集团也投资5000万美元风险基金资助区块链项目;杭州复杂美区块链研究中心也透露,目前正在与国内一些企业机构交流、合作、对接,致力于让区块链技术不再局限于研究阶段。

目前物联网存在很多问题，主要是成本过高、用户对其缺乏信任、没有实际的使用价值、没有可预期的商业模式等。隐私、安全和容错性是物联网发展的前提。那么区块链如何应用于物联网呢？

区块链记录了每一个参与者的每一笔交易。密码学被用于确认交易和保证区块链上信息的私密性。参与者确认每一笔交易，提供高度冗余的确认，同时还会因为付出了计算力，获得相应的奖励。通过使用去中心化的共识确认交易，区块链消除了对信任的需要。

尽管区块链作为长期的价值贮藏手段（例如比特币）可能会带来监管和经济风险，但是它作为一种交易处理工具是革命性的创新。在去中心化的物联网中，区块链是能够促进交易处理和交互设备之间协作的基础架构。每个区块链管理自己的行为，发挥自身的作用，这样就会形成一个“去中心化的自治物联网”，从而实现数字世界的民主。

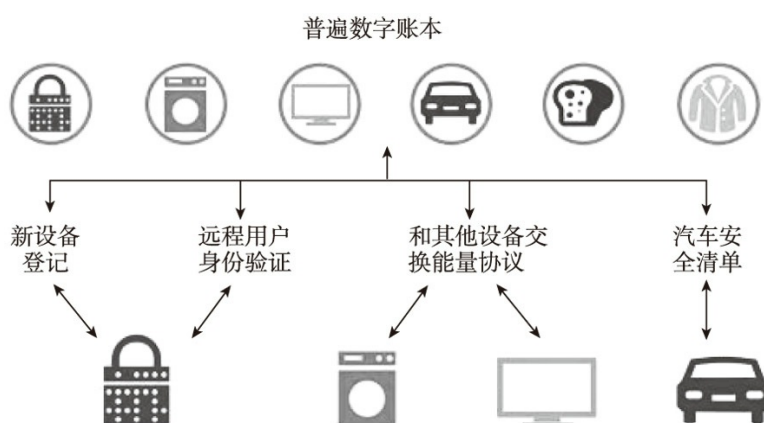


图4-3 区块链充当一个通用的数字账本，促进物联网设备间不同类型的交易

资料来源：<http://www.wanbizu.com/fazhan/201410122995.html>

当没有中心化的服务器充当消息中介、支持文件存储和转移、行使仲裁职能时，任何一种去中心化的物联网解决方案都应该支持以下三种基本类型的交易：无须信任的点对点通信、安全的分布式数据分享和强大的可扩展的设备协作方式。

安全的分布式文件分享协议具有取代基于云的文件存储和传输的潜力，实现安全的软件、固件升级和在设备间进行直接的文件分享。对物联网发展最大的挑战不是简单地建立一个去中心化的物联网，而是建立一个规模可以不断扩展的通用物联网，同时保证隐私、安全和无须信任交易。换句话说，物联网中数以千亿计的参与者不都是值得信任的，有些甚至是恶意者，所以需要某种形式的验证和共识机制。

聚沙成塔的分布式云存储

爱好摄影的李阿姨最近正被一件“大事”所困扰。李阿姨每年都会约朋友一起去国外旅游，拍摄了大量的照片留作纪念，并时常与朋友分享。平时李阿姨把照片存在电脑硬盘里，甚至不让老伴碰这台电脑，就是担心老伴不小心删除了她的“宝贝”，但是不幸的事情还是发生了。有一天当她打开计算机后，发现硬盘上的照片打不开了。她心急火燎地给电脑厂商打电话，厂商说硬盘早过了保修期，能不能恢复数据要看硬盘的受损情况，一周以后消息传来，硬盘数据已丢失，照片无法恢复。有没有一种办法，能解决李阿姨的问题，实现信息的安全、永久存储呢？

分布式云存储

答案就是分布式云存储。中心化的存储方式或多或少面临着信息安全和永久存储的问题，而基于区块链技术的分布式云存储将是解决这一问题的最佳方案。与目前中心化提供的云存储空间不同，基于区块链技术的分布式云存储不但可以储存，还可以同时证明这份数据是真实可信的，并且永远不会被修改。区块链的特点就是分区块存储的，每一块包含一部分交易记录。每一个区块都会记录着前一区块的ID，形成一个链状结构，因而被称为区块链，以此来保证每一个块上的信息都是不可更改的。区块链实际上就是一个分布式数据库，是加密后分散式存储的云存储。

基于区块链的分布式云存储主要具有如下特点：

1. 实现碎片资源的可利用

每个人都可以通过分享个人的硬盘空间获得金钱回报。这个金钱回报由租户直接支付给个人，提供服务的平台只收取微小的服务费。可以理解为平台就是硬盘存储的Uber。

2. 大众广泛参与

所有人都可以访问公开区块链上的数据，所有人都可以发出交易等待被写入区块链。共识过程的参与者（对应比特币中的矿工）通过密码学技术以及内建的经济激励维护数据库的安全。

3. 高效、低成本运行

区块链技术在网络上公开、透明、开源的。不需要通过任何的机构及组织，可以随时随地上传、下载所需要的信息。比起购买昂贵的存储设备及配套的人力来说，租用硬盘空间比较经济、实惠。

4. 较高的安全性

传统的云存储公司购买或租用服务器来存储他们的客户文件，同时使用RAID方案或多数据中心的方法来保护数据的安全性。而使用区块链技术不需要中心化，不需要购买昂贵的设备及维护人力。区块链技术让文件存在于一个分布式、虚拟和分散的网络中，这样就不需要像传统的云存储公司那样依靠硬件的维护来保证存储的可靠性。

中心化的云存储早已进入商业应用阶段，如亚马逊的云平台十分强大，足以让用户以平台为基础开发某些复杂度高得惊人的功能，支撑亚马逊云平台强大功能的就是百万级数量的服务器。根据2015年公布的数据，亚马逊在全球11个地区部署了服务器，每个地区建立了数个数据网络，全球共拥有28个数据网络。每个数据网络由一个或多个数据中心构成，通常配备5万~8万台服务器。据保守估计，亚马逊在全球范围拥有150万台服务器。市场研究公司Gartner的分析师估计，亚马逊的服务器总数达到200多万台。亚马逊的云平台庞大而复杂，几乎可以说，支持这一平台的数据中心可以构成地球上最大的计算机，从某种意义上讲，它就是一台通用功能的巨型计算机。报告显示，亚马逊云服务在全球云市场中占据了27%的份额，微软的份额约为10%，随后是IBM和谷歌。

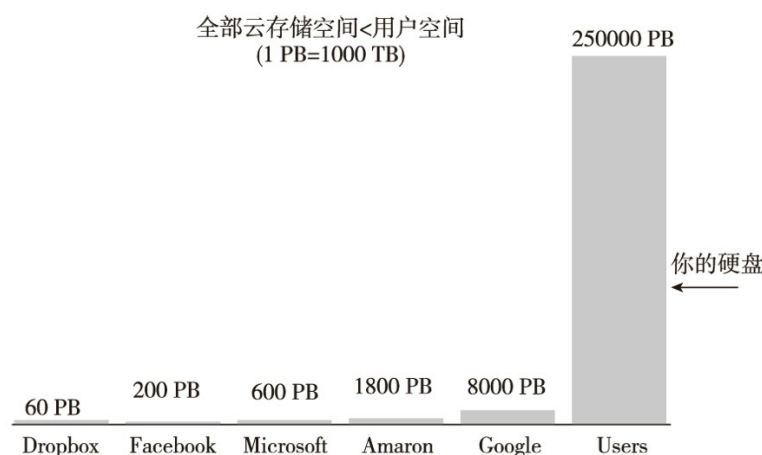


图4-4 云存储与用户空间的可视化

资料来源：<https://storj.io/storj.pdf>

从图4-4我们可以很容易看到，图表实心块是目前几家大公司所具有的存储能力，空心是我们现有的可以使用的存储空间。不论Facebook、Microsoft、Amazon，还是Google公司，服务器再多，再如何增加，都不能与我们现有的可以使用的免费的存储空间相抗衡。

我们可以畅想，电脑制造商们将会设计一款没有硬盘的计算机，因为好处是显而易见的，“我们的电脑不需要硬盘”光是这句广告语，就足以让“粉丝”们兴奋不已，不假思索地下单。“精明”的用户可以算一笔账，假如说我们买一台笔记本原来可能会花费1万元，但是没有硬盘的话，应该在8千元左右，而我们只需要再拿出很少费用租用一个云存储即可。

在区块链上提供去中心化云存储方案的有Storj公司。该公司组织的网络可以提供大约超过1500TB的存储空间，大约有430名“矿工”，它使用的“燃料货币”是Poloniex交易所上最古老和最有价值的币种之一。Storj是如何解决文件的存储、加密功能的呢？

图4-5清晰地解释了文件如何被存储。我们可以理解为文件被自动分解成字节，存在A\B\C三个不同的硬盘上，而私钥就在你自己手里，不论是提供服务的服务商Storj公司还是为你提供存储库的人都没有私钥，这就解决了信息被泄露的问题。还有一点，如果万一你的私钥不小心泄露，拿到私钥的人得到了你存在某个硬盘上的信息，这块信息也有可能是一段乱码，而不是一整篇文章。更让人惊叹的是依靠区块链技术我们还可以做到多重备份，比如上例中的李阿姨，她把照片上传后，还是不放心的图片存放在一个人那里，则可以在保存文件的时候，同时备份1份到6份，这可以理解为硬盘保护的“加强版”，当然所付的费用会高些，但是相对于购买昂贵的硬盘来说还是比较经济的。

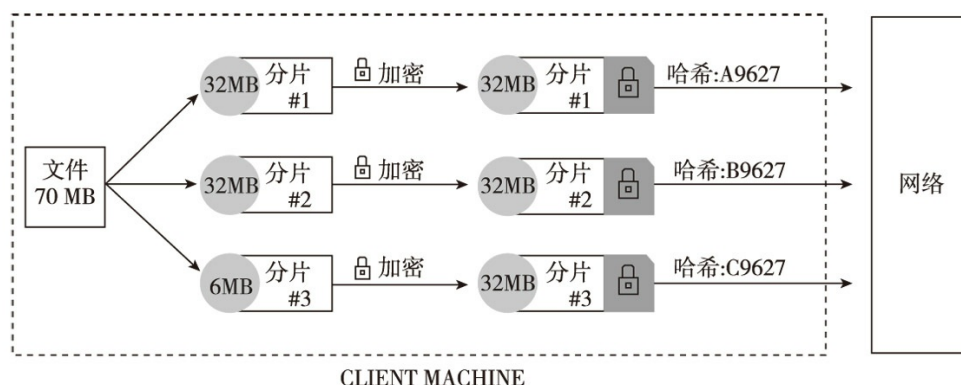


图4-5 切分过程可视化

资料来源：<https://storj.io/storj.pdf>

Storj在2015年11月28日发布了首个图形界面的版本，让普通人可以自由地分享他们的硬盘空间，而不需要任何特殊的IT技能。每个用户可以根据分享的免费空间来获得他们的SJCX，这取决于共享空间的大小和时间。SJCX是Storj网络系统中的一种代币，可以把它想象成一种“货币”。用户可以在指定的“商场”中使用和流通这种“货币”，也可以通过SJCX来租用或者购买存储空间。Storj公司从测试开始已经进行了4轮代币发送，大约发送出347000个SJCX，预计在测试结束前大概还会释放出80万个SJCX。

其他区块链相关服务

SIA、MaidSafe和以太坊也提供类似服务。

SIA是另外一个有趣的项目，该项目计划通过应用程序开发来整合存储能力。为此，它和去中心化的应用平台Cripty合作，实现能够让开发者写他们自己的应用程序这一目标。Cripty提供了一个真正基于区块链的，能够部署去中心化应用的完整解决方案，同时还提供了一个绝妙的用户体验，让任何人都可以在数秒内进行安全和简单的交易。但从现有进度来看，SIA项目还远远落后于Storj，即便它已经推出了图形界面客户端，但论坛上缺乏活跃用户，并且在Poloniex上对于SiaCoin的介绍也不是很好。SIA开始进入市场时价格大概是6900聪，目前已经下滑到5聪左右。

MaidSafe是一个开源项目，它声称会给世界带来一个“去中心化的互联网”。MaidSafe的团队有16名成员，据网站说已经在一起工作8年了。MaidSafe网络即将公开beta测试，将会在内部进行运作。该公司代码的主要部分将会在开源许可证的情况下进行下载。

以太坊也许是未来Storj最为危险的竞争对手，其已经发布了一个测试版本，称为Ethereum Frontier。以太坊目前在Poloniex交易所中是交易量最大的数字货币，并且目前整个项目看起来已经初具规模。它提出要建立“去中心化的软件平台”，能够让所有人在平台上进行构建自己的去中心化应用。以太坊还列出它的豪华合作伙伴阵容，目前没有任何团队可以与之匹敌，其中包括微软、IBM和三星。

自由交易：下一个阿里巴巴

经常有人说“阿里巴巴就是中国的亚马逊”。虽然两家公司都做互联网商业，但和亚马逊不同的是，阿里巴巴并不拥有其平台上销售的大部分商品，也并不用维护庞大的经销商中心，阿里巴巴的淘宝是为消费者提供直接和小商家联系的渠道，而其另一主要购物场景天猫则为消费者提供与较大品牌零售商的联系。阿里巴巴联合创始人之一马云就说过：“亚马逊和eBay是电子商务公司，阿里巴巴不是电子商务公司，而是帮助别人来做电子商务，我们不卖产品。”阿里巴巴的盈利模式主要是通过为零售商销售广告和搜索位置（有点像谷歌），以及从天猫上的较大零售商手中获取佣金（这点和eBay有点像）。

阿里巴巴的成功是无可厚非的，但是我们不难发现阿里巴巴的盈利模式是建立在对商户的有偿服务之上的，阿里巴巴从本质上来说是一个成功的“第三方中介机构”。那么，在互联网的世界里有没有一种不需要商业性质的“第三方中介机构”的平台，只通过买卖双方自己达成信任实现交易呢？

基于区块链技术的发展，在互联网的世界里有了这样一家这样的“公开市场”。它利用开源的点对点的技术，实现了买卖双方的直接交易，而不需要借助中心化的平台，信任、安全和纠纷处理都由系统来处理。在这个“公开市场”里面所有人都使用在线交易的新方式，通过在电脑上运行一个程序，你可以直接连接到网络的其他用户，并进行交易。这个网络不是由一个公司控制的，也不是组织管理的，而是去中心化商城，这意味着你不需要支付广告费用。

现在，电子商务意味着使用中心化的服务。eBay、亚马逊和其他大公司对卖家实施严格监管的同时收取不菲的费用。这些公司只接受像信用卡和PayPal这样的对卖家和买家都收取手续费的支付方式。它们需要用户的个人信息，这些信息可能被盗取或者卖给其他人，被用于精准投放广告或者危害更大的滥用。而“公开市场”是为网上点对点交易创建的去中心化网络的开源项目，买卖双方使用比特币进行交易，没有费用，而且公开个人信息的决定权在用户手中，为电子商务提供了另一种途径。

假如，你打算出售你的旧笔记本电脑。你需要首先下载客户端，然后在你的电脑上创建一个商品目录，并标明商品的细节。当你公布这一商品目录后，该目录被发送到“公开市场”的分布式网络上。其他用户搜索你设置的关键词：笔记本、电子产品等时，就可以发现你的商品目录。他可以接受你的报价或者提出新的报价。

如果你们两个人都同意这一价格，客户端就会使用你们的数字签名在你们之间创建一个合约，并将该合约发送到被称为公证人的第三方。当买卖双方产生纠纷时，公证人就介入交易。

这些第三方公证人和仲裁者也是网络的用户，可能是你的邻居也可能是地球另一端的陌生人。第三方为合约作证，并创建多重签名比特币账户，只有当集齐三个签名中的两个时，比特币才会被发送给卖家。

买家发送商定好的数量的比特币到多重签名地址。你会得到通知，知道买家已经发送货款，然后你就可以发货了，并告诉买家已经发货。几天以后，买家收到笔记本，他将告诉你收到笔记本，并从多重签名地址释放货款。你获得了比特币，买家获得想要的笔记本。没有交易费用，买卖双方皆大欢喜。

如果产生交易纠纷该怎么办？例如你从卖家手里买了一本书，你向多重签名地址发送比特币，但是他们发错了货，或者质量不像广告说的那样好，或者卖家根本没有发货，那该怎么办呢？这就需要第三方介入了。卖家只有在多重签名集齐三把私钥中的两把才能够从多重签名地址中取走货款。第三方公证人控制着第三把私钥，所以在买卖双方达成和解或者第三方认为卖家或者买家是正确的以前，多重签名地址中的比特币不会被移动。

开始时你怎么能信任第三方呢？在用户隐私不被公开的网络上，你怎么能够信任别人呢？“公开市场”平台有一个信誉评分系统，允许所有的用户对其他用户进行反馈评分。如果某些人打算诈骗其他的用户，他们的信誉将会受损，第三方如果不能公正裁定交易纠纷，他们的信誉也会受损。当你在平台上购物和选择第三方公证人时，你能够看到他们的信誉评分，判断其他用户是否信任他们。保证这些评分是合理的和防止作弊是巨大的技术挑战。

如果这样仍然不能消除你的疑虑，卖家和买家可以创建一个投票池，由买卖双方都信任的用户组成。这些步骤可能听起来很复杂，但是客户端会处理这些细节问题。它们的目标是为用户提供比陈旧的中心化平台更好的用户体验。

也有人会问，在这个如此自由的市场上你会交易什么呢？第一个猜测就是毒品。事实上，这种猜测是片面的。历史上第一笔电子商务交易是发生在斯坦福大学和麻省理工学院的学生之间。40年前，他们通过阿帕网（Arpanet）进行了一小笔毒品交易。如果我们因此而关闭了互联网，那么我们就无法体验到它为当今社会和商业带来的好处。

“公开市场”为消费者带来的好处是：更多的选择。消费者可以根据具体的需要选择阿里巴巴这样中心化的电子商务或者是去中心化的电子商务，从而迫使服务提供者向用户提供更好的价值定位。

OpenBazaar是一个功能齐全、面对全球用户免费使用的点对点市场平台，目标是建立一个去中心化的电子商务基础设施系统。OpenBazaar的创始人Brian Hoffman（布瑞恩·霍夫曼）指出，OpenBazaar的中心价值主张是：为交易双方提供不依赖于可疑中心服务机构的自由交易。项目小组会致力于推动该项目使用的合法化。

OpenBazaar已经发布了测试版。测试阶段平台只接受没有任何价值的测试用的比特币，希望开发者能够从中发现系统漏洞，尽量降低系统风险。该系统测试版下载次数高达19593次，首批商家零星出现，提供的服务也是参差不齐。很多急于加入平台的人已经等不及正式版本，下载了试用版并自担风险运行。与此同时，该平台进行了第一笔交易，涉及三个Super Bitcoiner钥匙链、BitAccess的区块链软件工程师ShayanEskandari、Reddit的作者Tyler Smith，后者还在平台上进行了另外两笔交易。从Sam Patterson那里购买了大头针，从该平台另一个联合创始人Brian Hoffman那里购买了一罐红牛。

当前，OpenBazaar项目所面临的最主要的问题是用户的非法交易，由于用户使用强加密软件Bitmessage、PGP以及数字货币，OpenBazaar将无法探听用户的交易。OpenBazaar也无法收集发生在平台上的活动的数据。OpenBazaar发布之前就因为潜在的非法交易可能性而被大量报道。Sam Patterson说：“我们预计OpenBazaar上的交易会反映整体社会面貌。只有很小一部分人进行不道德或非法交易，这不能阻止大多数正规交易的进行。”霍夫曼曾表示，他的团队不认可也不支持使用OpenBazaar用于非法目的，如果平台的大趋势是成为非法用途的温床，那他将远离这个项目。

在OpenBazaar的系统下进行交易也离不开第三方中介机构，但第三方中介机构在交易当中发挥的作用则完全不同于中心化的电子商务系统。独立公司OB1目前是OpenBazaar平台上完成度最高的第三方提供商。作为建立在OpenBazaar框架上的增值服务业务，OB1最初将专注于三个核心方面：

第一，主机解决方案。OB1正在与云服务器提供商数字海洋（Digital Ocean）进行合作，为其提供一个易于使用的第三方解决方案。

第二，仲裁服务。该公司希望提供标准合同服务，即在法院具有法律效力，尤其是对房地产等高端行业。它们的目标是为不同的需求、商品和服务提供一个合法的框架，以及不同的合同类型。

第三，买家保护。OB1的目标是提供第三方保存服务，以及为买家和卖家提供保险。

Bitcoin Full Node from Europe也是一家“公开市场”的第三方服务商，这个店出售比特币节点托管服务，为比特币支持者们提供帮助网络发展的渠道。店铺提供东欧国家服务器的全节点运行的比特币核心钱包（比特币官方钱包客户端）。目前提供的运行计划有三种，限时1个月、3个月或6个月；价格从0.0359~0.1029比特币。卖家称，在交易发生24小时内，会给买家全节点IP地址和一个监控数据的页面。

Jacob Ian Long和Esq是OpenBazaar上常见的商品担保交易服务提供者。支付该服务费的方式有两种：第一种是直接支付，这种方式只有在买家认识和相信卖家的区块链使用，否则会有

风险，和所有比特币交易一样，即使未收到服务或商品，也不会退款。另一种支付是担保支付（Moderated Payment），买家把钱转到代管账户，交易完成之后会进行支付。担保交易服务提供者不对交易成功做任何事，一旦发生纠纷，他会裁决失误方以及是否付款，这项服务是收费的，卖家和交易担保者都会有信誉评级。担保者进入平台的时候，OpenBazaar会预测其是否在现实中利用信誉获取信任，就像律师一样。

21 Inc: 共享经济的延伸

共享经济一般是指以获得一定报酬为主要目的，基于陌生人且存在物品使用权暂时转移的一种新的经济模式。共享经济的五个要素分别是：闲置资源、使用权、连接、信息、流动性。共享经济的关键在于实现最优匹配、实现零边际成本、解决技术和制度问题。共享概念早已有之，在传统社会，朋友之间借书或共享一条信息，邻里之间互借东西，都是一种形式上的共享，但这种共享受制于空间、关系两大要素，仅限于个人所能触达的空间之内。互联网技术的不断发展使得共享经济得以在更大范围实现。2010年前后，随着Uber、Airbnb等一系列实物共享平台的出现，基于中心化体系的共享经济模式得到了极大发展，而基于互联网通信和密码学技术发展起来的区块链技术对于共享经济有着更为天然的契合性，我们有理由设想，在去中心化的系统下，共享经济将向更广阔的范围延伸。

21 Inc是一家区块链创业公司，成立于2013年，位于旧金山。21 Inc的主要业务就是提供一款嵌入式芯片BitShare，允许用户使用智能手机和其他互联网设备进行比特币挖矿。21 Inc此前曾获510万美元A轮融资。

21 Inc推出了新产品Ping21，这是一个全新的技术概念。有了这个Ping21服务，网站管理员就可以使用一个命令，接收他们的网站在几十个不同国家的正常运行时间及状态信息。根据21Inc的介绍，每个电脑设备都会拥有一个自己的钱包，它可用于购买和出售数据。用户通过利用21Inc推出的微支付市场，将不需要支付昂贵的包月费，客户端只需要向网络提交一个请求，Ping21服务的比特币电脑会自动执行ping操作，检查网站，收集任何有必要的的数据，并将这些数据提交给用户，同时使用比特币进行付款。而且这个价格非常便宜，便宜到只需要0.00001个比特币。

2015年10月，21Inc推出比特币电脑并在亚马逊开售。仅需399美元，用户就可以购买到这款装载着定制芯片的小型比特币电脑，并可用其生产比特币。当然，能够生产出的比特币数量有限，事实上，根据计算，电脑在不间断运行的情况下一天仅能够生产出价值约为10美分的比特币。此外，生产比特币的能力还与你的居住环境有关，生产所耗费的电力成本可能会远远高于生产出的比特币的价值。该公司声称，有了这个平台之后，经济活动的发生就不再需要用户持有银行账户，或在交易过程中使用政府支持的货币，让用户与用户之间的自由交易变为可能。21 Inc的工程师表示，机器到机器端之间发送和接收比特币的能力具有潜力解锁一种新型的“机器经济”，其中机器能够定期地将数据和服务交易量化为比特币。“通过使用比特币微交易来激励机器操作者，我们就可以得到世界各地非常准确的实时网络状况数据”。另外，21 Inc销售的这款技术设备其实并不是他们最终计划向广大民众所开放的版本。事实上，这款电脑只是

在对21 Inc的技术进行证明，希望借此打动开发商，令其使用21 Inc的芯片来制造应用程序。在接下来的几年中，21 Inc预计这类芯片将会变得更小和更便宜，且可被内置于各式各样的第三方设备之中，就像今天的英特尔芯片一样。21 Inc的最终设想是把具有上述功能的芯片嵌入智能手机，届时wifi分享、慈善捐款、自动付费点唱机等都可以使用21 Inc的技术，未来其应用的范围将十分广大。

现在我们不论是进入餐厅还是咖啡馆，首先问的不是“有冰镇的可乐吗？”而是“请问，你们提供的免费wifi密码是多少？”有了这款芯片，手机将会根据你周围可提供的愿意分享自己wifi流量的号码，自动登录，并根据你所使用的时间和流量收费，对于分享者来说，一小点的分享也能带来一小点的回报，也是很不错的选择。

你可能在电视上、网络上看到一条令你心碎的消息，你只要发短信到某某电话号码，即可向特定的慈善机构捐献10美元，而慈善机构将把你的捐款转给受捐人，以期给他（她）们的生活带来帮助。在这项交易中，电话运营商充当了中间人，将10美元纳入了捐款人下月的电话账单中。这种服务会给客户带来诸多方便，如果客户想捐款，不需要从包里掏出信用卡，也不需要担心自己的信用卡会因此遭盗用。

使用这项技术的其他产品也将能通过类似的方式运营。市场上可能会出现这样一种照相机，可以在内部存储量不足的状态下自动购买在线存储空间以继续拍摄照片和视频；也可能出现这样一种平板电脑，可以自动检测出可供租用的wifi网络，并以价值若干便士的比特币购买到wifi的使用权。

除此之外，也许商家会为虚拟货币的使用想出一些其他巧妙的方式，令消费者的生活更加方便。同时，伴随着人们家庭中和工作场合里数字设备数量的不断增加，21Inc的这项技术也有助于解决“孤儿设备”的问题。在此之前，原始的研发公司停止了对某些数字设备的支持和维护，而任由其处于损坏或者更糟的不安全状态下。如果用户为每个这样的“孤儿设备”缴纳少量的比特币作为维修费，无论其设备制造年限多长，21Inc都将为原始制造商们继续提供支持和维修设备的基金。

如此，你可能仍会感到奇怪，为什么人们要购买这样一个奇怪的“印钞”芯片来替代实际金融系统进行日常买卖的支付？以下是两大原因：原因之一是，对于某些应用程序而言，用户将信用卡的信息输入某种特定的数字设备中具有一定危险性。而一个更加根本的问题是，传统金融系统中有关手续费用的规定令小额交易非常不划算。在信用卡的花销机制中，用户进行的交易额越小就意味着手续费在交易额中占据的比重越大。这就是为什么我们在网络商店中很少看到有比iTunes商店里99美分的歌曲还要便宜的东西。在低于1美元的经济维度下，信用卡支付功能几乎已无法发挥其效用了。而小额交易才是21Inc能发挥其“魔力”的领域：也许标准的比特币网络并不是一个良好的小额支付平台，但它却是一个无比开放的软件平台。而公司也已经研发

出了新技术，可令比特币网络内的小额支付比其他任何一种在线支付技术都更具效率。小额支付还可运用于其他领域：用“小额”的比特币支付英文对中文的翻译或文件的转换；建立自己的数字商品商店，类似iTunes；租用物联网硬件设备，从智能密码锁到3D打印机；运用机器人查找哪家网站上的手机最便宜；购买喜欢的音乐；为邮件付费，减少垃圾邮件的产生；减少网站的广告（现在网站的经营者只能靠收取广告费来赢利）。

但是，如果你仔细想一想这种数字设备在实际生活中的工作原理，就可以清楚地看到，推广这种技术仍然存在着很大的困难。想象一下，在未来你的家中装满了内置21Inc比特币“挖矿”芯片的家用设备，而在月末你突然发现，电费比你所预期的高了20美元。也许是因为当月天气炎热，你的空调“加班”运行了多时；也许是你的比特币设备遭遇了黑客袭击，有坏人偷走了你的电力为他们自己生产比特币去了；又也许是你处于青春期的儿子最近新买了一个设备，该品牌不在比特公司名单上，因此在生产出大量比特币的同时也耗费了超于其所承诺的更多电力，额外的附加费用都交回了原始的制造厂商。问题在于，你永远不会得到答案，也不存在一个简单的方式能够找寻到这一问题的答案。这不像是你的电费账单明细，能将各式电器所耗费的电量逐一列出。如果你使用了比特币设备，你将会被迫开始自主测量房内各种家电的能耗，这种计算上的麻烦是21Inc应当考虑进行消除的。

第五章

区块链应用的全球进展

区块链以一种去中心化的方式集体维护一个持续生长的数据库，为金融业的未来升级提供了一个可选的方向，因此也吸引了全球金融巨头和投资人的目光。

根据区块链科学研究所创始人梅兰妮·斯万的观点，区块链技术发展分三个阶段或领域：区块链1.0、2.0和3.0。所谓区块链1.0，就是数字货币领域的创新，如货币转移、兑付和支付系统等；区块链2.0更多是做一些合约方面的创新，即商业合同涉及交易方面的，比如股票、证券的登记，期货、贷款的清算结算，所谓的智能合约等；区块链3.0则更多地对应人类的组织形态的变革，包括健康、科学、文化和基于区块链的司法、投票等。

目前区块链技术的发展和主要应用处在对区块链1.0和区块链2.0的探索阶段。与此同时，世界各大金融机构都在紧锣密鼓地向区块链技术的研究和区块链项目投入资金，其中就包括纳斯达克、高盛、花旗银行、摩根大通、瑞士银行、道富银行、桑坦德银行、巴克莱银行等。

2015年上半年，比特币公司coinbase、21 Inc和Circle接连获得美国风险投资公司Andreessen Horowitz、芯片制造商高通公司（Qualcomm）、纽约证券交易所（NYSE）、金融巨兽高盛等巨头公司的注资，三家创业公司共计获得2.41亿美元巨额融资。

进入2015年下半年以后，区块链概念开始兴起，传统金融巨头也开始尝试布局区块链或分布式账本项目。据统计，在2015年，非比特币区块链领域投资事件共13起，占比19%；投资额1.293亿美元，占总投资额的23%。

吸引投资和合作伙伴最多的当属分布式账本技术即区块链技术初创公司R3CEV，其主要致力于为银行提供探索区块链技术的渠道以及建立区块链概念性产品。以R3CEV公司为核心的区块链联盟于2015年9月成立，截至2016年初，共有42家金融机构成为其创始伙伴。

目前，R3CEV联盟已经完成了两轮金融机构大规模参与的测试。按照各方分析人士的观点，R3 CEV倡导的区块链技术可能很快会应用于国际金融支付和清算领域，首先颠覆现有的支付系统。

2016年以来，越来越多的创业者与机构开始重视区块链技术。107个项目、29个投资事件、24127万美元的投资额（数字仍在变动.....）。在区块链应用方面已经取得进展的主要有以下项目。

BitPay融资3000万美元，估值达1.6亿美元

日期：2014年5月9日

公司: BitPay

金额: 3000万美元

轮次: A轮

地区: 美国亚特兰大

投资方: Index Ventures、理查德·布兰森 (Richard Branson)、雅虎联合创始人杨致远

比特币商业交易平台BitPay进行的一轮融资已经筹得了3000万美元资金, 该金额是截至2014年5月该领域规模最大的一轮投资, 现在该公司的估值大约为1.6亿美元。加上前一轮的融资, BitPay获得的投资额已经超过了其他竞争对手。

这也是比特币生态系统变得成熟完善的标志之一, 许多顶级风投公司都开始向这一领域投入大量资金。虽然之前出现了Mt.Gox破产这样的严重事故, 但是大型投资基金都想在该领域投入至少一家公司, 准备迎接比特币的重新崛起。

BitPay在2013年处理的交易金额超过了1亿美元, 还获得了Horizons Ventures的投资, 这是香港亿万富豪李嘉诚旗下的投资公司。BitPay之前已经跟Zynga和Branson等客户进行了一些大型的比特币支付测试。BitPay的交易平台主要面向中小型的企业, 它通过提供不同等级的账户获得收入, 不同账户等级的收费从20美元到300美元不等, 除此之外还有其他定制功能的账户等级。它还提供了一个入门交易套餐, 对所有的交易都只收取1%的手续费。

Coinbase正式完成7500万美元C轮融资

日期: 2015年1月20日

公司: Coinbase

金额: 7500万美元

轮次: C轮

地区: 美国加州

投资方: DFJ Growth、Andreessen Horowitz、Union Square Ventures、Ribbit Capital、NYSE、财富500强金融服务集团USAA、西班牙对外银行BBVA以及日本电信巨头DoCoMo

比特币支付处理商Coinbase于2015年1月20日正式完成7500万美元C轮融资。此轮融资也标志着此前由blockchain.info所创造的单笔3050万美元融资纪录作古。

Coinbase首席执行官Brian Armstrong（布莱恩·阿姆斯通）认为参与此轮融资的投资者们对于比特币行业的创新都感到非常兴奋，他们希望能够利用投资Coinbase的方式，来了解比特币更多的可能性。

Coinbase用这笔新融资扩张员工数量的同时，还注重提高他们的移动端产品质量，此外Coinbase还打算向发展中国家扩张，将着重关注全球范围内那些没有银行服务的地区。而Coinbase的这笔7500万美元融资，是截至2015年1月比特币行业里融资规模最大的一次。

Coinbase会根据客户的需求调整其产品，将其APP翻译成各种语言版本，此外有了这一大笔资金，Coinbase就无须再为监管负担而烦恼。Coinbase拥有了超过200万数量的钱包用户，而公司的数据指标表明，用户的增长其实与比特币价格所呈现的关系不大，而投资者们实际上也并不关心Coinbase当前的用户数量，他们是将重点放到长期内Coinbase将会发展到何种地步。

超越Coinbase，初创比特币公司21 Inc获1.16亿美元巨额融资

日期：2015年3月11日

公司：21 Inc

金额：11600万美元

轮次：C轮

地区：美国

投资方：领投者包括美国风险投资巨头Andreessen Horowitz、RRE Ventures、来自中国的私募股权公司Yuan Capital、芯片制造商高通公司，其他投资者包括Khosla Ventures、Data Collective、PayPal联合创始人彼得·泰尔（Peter Thiel）、马克斯·列夫琴（Max Levchin）、eBay公司联合创始人杰夫·斯科尔（Jeff Skoll）、Dropbox公司首席执行官德鲁·休斯顿（Drew Houston）、Expedia首席执行官达拉霍斯劳沙希（Dara Khosrowshahi），以及Zynga公司联合创始人马克·平卡斯（Mark Pincus）

据华尔街日报2015年3月报道：在过去的一年半中，一家硅谷比特币初创公司暗中尝试说服

一些大腕风险投资者投资该公司，希望以此能将比特币技术带入大众市场。

这家名为21 Inc的公司终于浮出了水面，并宣布已获得了1.16亿美元的巨额风险投资，超越Coinbase成为有史以来数字货币领域内获得最多融资的初创公司。21 Inc联合创始人兼首席执行官马修·波克尔（Matthew Pauker）希望公司在较短的时间内能在软件和硬件产品领域有一些有趣的发展，以推动主流社会接受比特币。同时，高通公司的参与将是关键，可能会促使21 Inc将目光投向物联网市场。此外，21 Inc的前身是21e6（寓意比特币总量为2100万个），早在2013年11月时，21e6公司就在首轮融资中获得505万美元资金。

智能合约平台Symbiont获700万美元融资

日期：2016年1月

公司：Symbiont

金额：700万美元

轮次：A轮

地区：不详

投资方：不详

Symbiont这家智能证券交易平台完成了一轮700万美元的融资，该公司的估值已达到了7000万美元。

Symbiont起源于Counterparty（合约币）项目，它是由Overstock.com公司旗下Medici项目（现t0）的前成员创立的，根据Symbiont公司的网站介绍，“Symbiont正在建立第一个用于发行区块链智能证券和交易智能证券的平台”。智能证券是一个描述智能合约的术语，其可用特定的规则进行编程。

Symbiont的创始人是Robby Demody、Evan Wagner和Adam Krellenstein，2015年3月，三人所创立的Counterparty与Mark Smith的Money f（x）公司进行了合并。

Counterparty是早期的Bitcoin 2.0项目之一。在本质上，它可以允许用户执行不同的金融应用，而不仅仅是比特币的P2P支付网络，并且它也受到比特币网络的保护。此前，这家公司在种子轮中融得了125万美元。

“看到更多的风险资本进入这个领域，这是很好的现象，这代表了区块链解决方案有了更多更好的机会。但是，我们不能把融到多少钱作为一个成功的标志。我们会看到，一些公司仅仅融了很少的钱，却做得非常好，也有一些公司融到了一大笔钱，最后却失败了。我们更应该专注于理解部署、使用 and 实际客户创新的状态，以评估区块链对金融服务的影响”，虚拟资本风险投资公司（Virtual Capital Ventures）普通合伙人William Mougayar（威廉·穆贾雅）的这个观点算是对一些区块链项目的一个客观的评价。

比特币区块链应用公司**PeerNova**融资**860**万美元

日期：2014年12月

公司：PeerNova

金额：860万美元

轮次：A轮

地区：美国奥斯丁

投资方：此轮融资是由Mosaik Partners领投，AOL前首席执行官Steve Case（史蒂夫·凯斯）以及Crypto Currency Partners也参与了融资

比特币挖矿以及区块链软件解决方案初创公司PeerNova成立于2014年5月，是由矿业公司HighBitcoin以及CloudHashing合并而来，此前，HighBitcoin负责生产挖矿硬件，而CloudHashing则从事于销售挖矿云算力。

PeerNova的总裁兼首席执行官Emmanuel Abiodun（依曼尔·阿宾德）表示：“我们仍旧会继续挖矿，但它不会成为我们的主导业务，我们的定位更趋向于基础设施提供者，而非加密货币公司。”该公司的新网站进一步表明，去中心化的应用（DApps）、智能资产、智能合约以及电子货币软件应用程序将是PeerNova主推的新方向。

Abiodun提到了以区块链技术为基础的文件存储、身份管理以及资产安全传输等产品，他表示：“我们的根就是源于加密技术，我们正在使用这些技术帮助比特币成长，而不仅仅是作为一种货币。”

目前，有很多公司正在建立相关产品，旨在解锁比特币区块链以及竞争链，用于公众证明以及资产传输。对于许多初创公司而言，他们要思考的是，比特币技术不仅仅是应用于金融创

新，例如智能合约就是建立于区块链技术，它的策略将使得比特币不仅仅是一个货币。此外，Blockstream刚刚融资2100万美元，将用于打造侧链，新的竞争链将与比特币区块链建立联系，这对数字货币实验将产生重大影响，全新的公共总账应用正在建立。而PeerNova未来的业务正是朝着这个商业模式前进，Abiodun表示：“我们的重心就是在区块链之上创建软件堆栈。”

智能合约交易平台**Mirror**获A轮880万美元融资

日期：2015年6月

公司：Mirror

金额：880万美元

轮次：A轮

地区：美国加州

投资方：Route 66 Ventures在此轮融资中领投，其他跟投方包括巴特利风险投资公司（Battery Ventures）、交联资本（Crosslink Capital）、RRE Ventures以及蒂姆·德雷珀（Tim Draper）。此外，Route 66 venture合伙人帕斯卡尔·布维尔（Pascal Bouvier）将加入Mirror的董事会

Mirror公司的首席执行官艾维许·巴阿玛（Avish Bhama）认为，当前金融服务行业正发生着一场变革，Mirror公司看到了一个巨大的机遇，将为风险管理与套期保值提供更先进、更高效的服务。

2015年5月，Vaurum（Mirror公司的前身）获得了400万美元的种子资金，投资方包括Battery Ventures公司，蒂姆·德雷珀以及AOL首席执行官史蒂夫·凯斯（Steve Case）。

在完成此轮融资后，Mirror公司获得的总融资额达到了1280万美元，该公司表示，将利用这笔资金建立工程团队并拓展其国际业务。

区块链公司**Chain**获3000万美元融资

日期：2015年9月

公司: Chain

金额: 3000万美元

轮次: B轮

地区: 美国旧金山

投资方: Visa公司、纳斯达克、花旗风投、RRE Ventures、第一资本金融公司、Fiserv公司、Orange SA等金融巨头

旧金山区块链初创公司Chain的首席执行官Adam Ludwin（亚当·路德文）表示：“智能的区块链网络能够从根本上改善资产的移动，很高兴我们能够与这些机构进行合作，我们相信，他们能够充分利用这场即将到来、不可避免的市场格局变动。”

支持Chain公司的投资方还承诺共同成立一个“区块链工作组”，以促进对区块链应用持续和定期的讨论。该工作组预计每年举行两次会议。此外，该公司还表示，RRE Ventures首席执行官吉姆·罗宾逊三世（Jim Robinson III）将加入公司的董事会，而Ludwin也将担任RRE的负责人。

Chainalysis募集160万美元的资金，与欧洲刑警组织签署网络犯罪协议

日期: 2016年2月

公司: Chainalysis

金额: 160万美元

轮次: 天使轮

地区: 不详

投资方: Point Nine Capital、TechStars、数字货币集团（Digital Currency Group）、Fundersclub和Converge VP

区块链初创公司Chainalysis已经与欧洲刑警组织的欧洲网络犯罪中心（EC3）签署了谅解备忘录，以后会共同努力打击网络犯罪。这个谅解备忘录签署的时间恰逢公司结束由Point

Nine Capital风投公司主导的160万美元的种子期资金。

Chainalysis的首席执行官Michael Gronager（迈克尔·格朗格）在一份声明中说：“这种新型合作是努力将数字货币从犯罪分子手中摆脱，移入消费者和繁盛商家手中的重要一步。”虽然大家普遍认为区块链技术在许多不同的应用和行业方面具有重大突破潜力，但Chainalysis公司认为，这种积极性一直受到负面新闻的影响，其中数字货币技术的应用与欺诈和网络犯罪有关。

好莱坞长老会医疗中心（Hollywood Presbyterian Medical Center）的敲诈事件就是一个典型事例。应数百万人的要求，医院最终被迫向黑客支付了1.7万美元，重新要回了其计算机系统的控制权。Chainalysis公司还引用了欧洲刑警组织2015年发表的报告，其中提到了网络犯罪正迅速增长，比特币也正在通往数字罪犯的路上。

Chainalysis公司通过跟踪区块链上数字身份改变的这种状况，表示其软件能够实时监测可疑活动，并提供帮助执法机构工作的调查工具。很多黑客活动是通过有关比特币交易元数据的私有数据库完成的。从这一点上来讲，黑客是最脆弱的。

值得注意的是，Chainalysis公司是越来越多的开发区块链合规解决方案的企业之一，其竞争对手包括Polycoin和Coinalytix这样的初创公司。

当黄金遇见区块链技术：**BitGold**获350万美元A轮融资

日期：2014年12月

公司：**BitGold**

金额：350万美元

轮次：A轮

地区：加拿大多伦多

投资方：PowerOne Capital、Soros Brothers Investments、Sandstorm Gold、PortVesta Holdings

加拿大数字货币创业公司BitGold总部位于多伦多，提供了一个专注黄金，以消费者为中心的互联网平台，用于全球区块链支付，同时提供安全、可赎回的黄金存储。BitGold公司认为自己的使命是：黄金安全存储及交易的全球入口，同时提供基于区块链技术的数字支付。

BitGold公司将黄金——比特币所设计模仿的一种资产，作为其中的一个重要元素。BitGold平台的灵活性将使黄金成为一个核心储蓄账户以及数字货币，形成无缝全球支付，或为一个必然发生的货币的互联网，提供一个自然世界的存储和安全阀。

BitGold公司的首席执行官Sebag（赛巴格）认为，区块链和Ripple等去中心化支付技术的突破，已经创建了一个历史性的机会——使黄金成为一种有效的日常交易支付方式。当还是一个专业投资者时，Sebag很好奇为什么会没有一种“拥有黄金”的简易方式，以及合法、透明、税务合规的花费黄金的方式。“真正的”黄金所有权，要求这个贵金属安全存储于地窖或保险柜中，这让其极难被花费，特别是在微交易中。但是BitGold通过开发一个平台解决这个问题——一部分黄金交易所、一部分支付技术、一部分托管，最终将形成一个非常好的用户体验，将黄金从一个物理元素提升为一个可用于互联网的，即时易得的记账单位以及价值存储手段，这将是一个黄金操作系统。

Align Commerce获1250万美元A轮融资

日期：2015年11月

公司：Align Commerce

金额：1250万美元

轮次：A轮

地区：不详

投资方：谷传奇投资公司凯鹏华盈（KPCB），跟投方包括数字货币集团（Digital Currency Group）、FS创投（FS Venture Capital）、Pantera资本（Pantera Capital）、征募创投合伙人（Recruit Ventures Partners）以及硅谷银行的投资部门SVB风投（SVB Ventures）

创业公司Align Commerce是由西联汇款前总经理Marwan Forzley（马万·弗斯利）一手创立，该公司正在寻求颠覆小型企业（SMB）的跨境支付市场。在加盟西联汇款之前，Forzley还是支付创业公司eBillme的创始人，后来西联汇款收购了这家创业公司，Forzley也因此加入了西联汇款。

Forzley表示：“我们相信跨境支付格局将被打破，采用新的技术可以帮助减少一些摩擦，这就是为何我们会用区块链。”Forzley声称其公司产品改进了传统电汇的跨境交易，这种解决方案

带来的不仅是成本上的降低，还有其他方面的益处。

Align Commerce公司还在2015年4月获得了一笔种子资金，但并未公布具体的金额，而最新获得的A轮融资将用于扩展Align公司的服务范围。而作为交易的一部分，凯鹏华盈的一般合伙人Randy Komisar（元蒂·克姆斯塔）将加入该公司的董事会。

Align Commerce使用区块链技术，是要取代代理银行在跨境支付过程中进行的工作。该公司认为，这种技术可以为商家客户提供更为经济的交易。其市场定位类似于分布式支付协议提供商Ripple。2015年10月，Ripple公司宣布将其重心放到跨境支付上。

这两家创业公司之间并没有争用相同的客户群体，尽管他们在技术方法上有着很大的相似性。Ripple的目标是银行，而Align Commerce瞄准的则是小企业市场。Align Commerce当前所使用的是比特币区块链，同时，如果有需要的话，Align Commerce公司的产品也可以使用Ripple的分布式总账。Align Commerce公司的产品是一个应用层的产品，可以切换到任何的加密货币。

比特币公司Blockstream斩获A轮5500万美元融资

时间：2016年2月4日

公司：Blockstream

金额：5500万美元

轮次：A轮

地区：美国旧金山

投资方：领投方分别是安盛战略风险投资公司（AXA Strategic Ventures，法国跨国保险公司安盛集团的风险投资部门）、Digital Garage（由伊藤穰一联合创立的东京在线支付公司）以及香港风险投资公司Horizons Ventures。其他参投方还包括AME云创投、区块链资本（Blockchain Capital）以及未来\完美风投（Future\Perfect Ventures）

Blockstream两轮融资共计拿到了7600万美元。迄今为止，该公司的标签技术一直是它的侧链产品，目前它正处于测试当中，这种技术可以将资产从一个区块链转移到其他的区块链。

而鉴于私链和许可管理（permissioned）区块链最近引起的关注，Blockstream尝试的可互操作区块链将为比特币网络添加功能性。

Blockstream首席执行官Austin Hill（奥斯汀·希尔）说：“我们是首批描绘可互操作区块链愿景的公司之一，也就是说将来不止会有一个区块链，而是会有很多的区块链。”不过，Hill表示公司仍会致力于开发开源比特币区块链的技术，他称之为“最成熟、最安全”区块链服务的基础设施。“我们不想看到的是，如果人们转移到了不同的协议和技术栈，最强大和最安全的区块链协议却遭到了淘汰，我们相信，所有这些区块链变得可互操作将是有利于社会的。”

Hill还引述了区块链创业公司数字资产控股（DAH）使用Blockstream技术的决定，以此作为开放式账本项目（Open Ledger Project）的一部分。这一开源区块链计划是由Linux基金会负责监督的，这也是比特币代码库对商业应用越来越重要的一个例子。

本轮融资紧随了数字资产公司的6000万美元融资。一方面，数字资产公司的许可管理或私有区块链解决方案，吸引了14家主流银行和IBM的注意，而Blockstream本轮融资的参与者大多数是风险投资公司，并且其技术目标所针对的是比特币网络。不过，在Hill看来，这些私链公司并不是Blockstream的竞争者。Hill表示，“有些时候，我们会争取机会，但我们也和数字资产公司的朋友合作。他们会对我们的代码进行反馈，我们已经和他们有过会面，并展示了通用架构。有迹象表明，他们正在关注的焦点并不是我们所专长和关注的。我们很高兴看到区块链在银团贷款方面的应用，但我们有着一个完全不同的背景。”

本轮融资对于整个比特币生态系统而言，将意味着一张信任票，Hill认为比特币的基础代码将被广泛使用，甚至是私有或许可管理的区块链解决方案。比特币是目前最成熟的区块链协议，它已经运行了一个价值20亿~70亿美元的安全赏金，多年来它已经给予了人们很大的信心。

区块链创业公司**Gem**完成**710**万美元**A**轮融资

日期：2016年1月7日

公司：Gem

金额：710万美元

轮次：A轮

地区：美国加州

投资方：本轮领投方为Pelion风险投资合伙公司，跟投方包括KEC风险投资公司、区块链资本、数字货币集团、RRE Ventures、Tamarisk Global、Drummond Road Capital、Tekton

Ventures、Amplify.LA、Danmar Capital以及天使投资人詹姆斯·华金（James Joaquin）

加州创业公司Gem至今共计融得资金1040万美元，前一轮330万美元的融资是在过去两年中完成的。作为交易的一部分，Pelion风险投资公司的合伙人本·达尔（Ben Dahl）将加入Gem的董事会。

Gem公司表示，公司此前为比特币开发者推出了多重签名API，目前他们正在扩大API开发，为区块链应用开发一个模块化平台可应用到多个行业。“我们相信，区块链技术将改变人们和企业之间的相互作用”，Gem首席执行官兼创始人Micah Winkelspecht（米克·威克皮特）说，“这将支撑整个行业，有一天将产生一种区块链经济，这将成为我们日常生活的基本架构。”此外，Bitium公司的首席执行官Scott Kriz（斯科特·科瑞兹）也被任命为Gem的董事会成员。

去中心化淘宝OpenBazaar获得100万美元种子投资

时间：2015年6月11日

公司：OpenBazaar

金额：100万美元

轮次：天使轮

地区：未知

投资方：风投公司Andreessen Horowitz、Union Square Ventures以及天使投资人威廉·穆贾雅（William Mougayar）

OpenBazaar旨在实现更广泛的P2P电子商务，使用比特币作为交换媒介，消除中心化模式导致的隐私和经济问题。

OpenBazaar最初是建立在Darkmarket这个去中心化市场上的，2014年4月在多伦多比特币世博会上赢得黑客马拉松比赛，后来从Darkmarket中分离出来。时隔一年，OpenBazaar宣布了这次的融资消息，此前OpenBazaar已经发布了几个测试版本，最新版本被称为“PortoBello”，在2015年4月下旬推出。

这些资金将被用来支付几个全职开发者的工资以及OB1的创建。OB1是一个新的公司，今后将会为OpenBazaar的用户服务。Union Square Ventures投资公司的管理合伙人布拉德·伯翰

（Brad Burnham）说，他的公司会支持这种区块链相关的创新项目，创新的关键是“开放市场”。他认为OpenBazaar的服务是一种新的共享公共数据层，将减少公司与客户之间存在的贸易壁垒，“有一些公共公司会为这一领域建立一些基础设施，我们会对这样的公司进行一些投资，OpenBazaar就是其中之一”。

穆贾雅和伯翰都认为OpenBazaar的发展及其去中心化商业的基础理念都与比特币和区块链的发展密切相关。支持该项目的人说他们不支持该技术被非法贸易利用，因为OpenBazaar的去中心化市场理念会促使人们将其作为暗网市场，最终会像“丝绸之路”那样衰败。伯翰承认该协议确实可以支持暗网市场的运营，但他指出OpenBazaar的开发人员对此不感兴趣。

高盛、IBM追投，区块链公司DAH融资6000万美元

日期：2016年2月

公司：DAH

金额：6000万美元

轮次：A轮

地区：美国纽约

投资方：高盛、IBM、荷兰银行、埃森哲、澳洲证券交易所、法国巴黎银行、Broadridge的金融解决方案部门、花旗银行、CME Ventures、德意志交易所集团、ICAP、桑坦德风投、证券托管清算公司（DTCC）、PNC金融服务集团

纽约区块链创业公司数字资产控股公司（Digital Asset Holdings）确认了投行界巨无霸高盛和蓝色巨人IBM也加入了其最近的一轮融资，这使得这轮融资的总金额上升到了6000万美元。

在这之前，该公司正在和摩根大通合作开展区块链试验项目，现在它已经获得了14家金融机构的支持。这轮融资也标志着高盛参与比特币和区块链领域的第二笔公开投资，上一笔发生在2015年，高盛领投了比特币服务提供商Circle的5000万美元融资。

高盛全球联席技术主管保罗·沃克（Paul Walker）在一份声明中说道：“我们相信，分布式账本技术在金融机构的全球范围交易中将扮演一个变革性的角色，我们期待着与数字资产公司以及更广泛的金融和技术社区一起参与这一新兴技术。”而蓝色巨人IBM则是首次公开披露投资一家区块链公司，目前IBM在开放式账本项目（Open Ledger Project）当中扮演了一个主导角

色，这一开源计划的参与者还包括数字资产公司。

“我们很高兴能够携手开发分布式账本技术，这将允许客户来转变他们的业务，并进一步加强我们和数字资产公司的合作伙伴关系。”IBM区块链研究负责人Jerry Cuomo（杰瑞·库姆）表示，他还补充说：“区块链拥有真正转变广泛行业的潜力，而IBM也将致力于使之商业做好准备。”

用区块链技术买东西？Colu获250万美元融资

日期：2015年1月

金额：250万美元

轮次：A轮

地区：以色列

投资方：Aleph Capital、Spark Capital、BoxGroup以及Bitcoin Opportunity Fund参与了本轮融资

以色列初创公司Colu于2015年1月宣布获得250万美元融资，这家公司旨在通过区块链技术来分配物品的所有权。其实就是可以使用代币（token）来交易任何东西，包括汽车、艺术品及演唱会的门票。比如说你买了一场演唱会的门票，一般而言你拿到的会是一张打印出来的门票，但是现在你收到的将是一串随机数（一张加密令牌）用于验证你购买了门票，而它们是通过区块链来实现的。你将得到一组私钥，然后你就可以访问到自己的门票。Colu会将这个代币置入一个二维码内，你可以通过自己的手机扫描后访问。因为它是数字的形式，你也可以将其传递给别人。

Colu自称比特币2.0，将集成多种服务和应用，能够让人们在区块链上购买和存储商品。Colu的创始人最初从ColoredCoins.org起手，这是一个为比特币区块链创建数字资产的开源标准协议。Colu就是基于这种想法的延伸，它既是开发者的API工具，也是一种应用，可以让消费者访问现有比特币框架上的彩色币（ColoredCoins）。它可以允许你在线购物，然后通过区块链进行验证。

Colu的创始人Amos Meiri（阿莫斯·梅瑞）表示：“当你买了艺术品后，你将得到一个基于区块链技术的代币证书，而这种数字证书将比纸张证书保存的时间更为持久。”

附录 区块链技术名词与核心原理

一、区块链的技术要素

（一）区块与链

从技术角度看，区块链是一种利用去中心化和去信任的方式集体维护一本数据簿的可靠性的技术方案。该方案要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（block）的每个数据中都包含了一定时间内的系统全部信息交流的数据，并生成数据指纹用于验证其信息的有效性和链接下一个数据库块。首先来看基于公有区块链讲解的两张图：

在图1中存在一个中心机构O，所有的节点要参与交易必须通过中心机构O来达成交易。

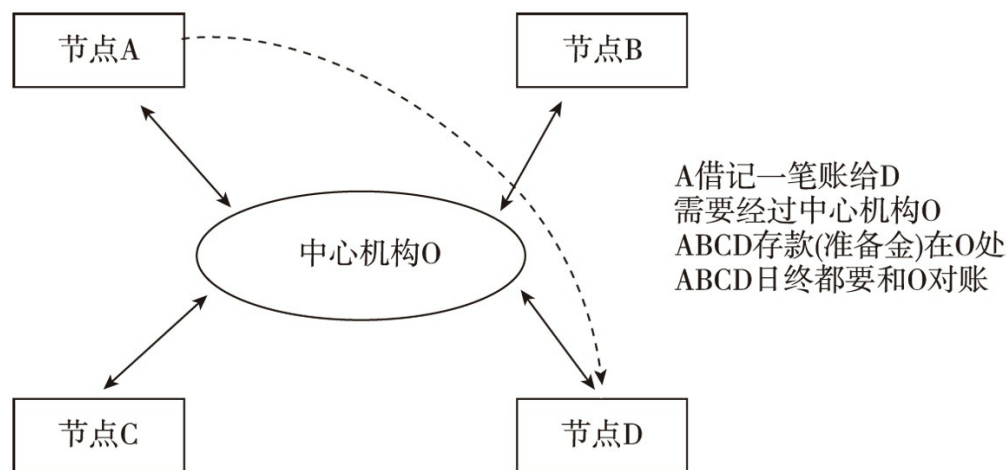


图1 区块链原理介绍1

这里的中心机构O扮演了两个身份，一个是维护者的身份，即维护交易账目正常达成且真实可靠；另外一个特权参与者的身份，即发行货币（资产）的权利。

如果我们要去中心化，那么我们应该如何做？

第一是去掉维护者这个身份，如何去掉它又能保证交易正常完成且真实可靠呢？首先，在区块链上我们只记录交易本身，而不是记录每个人的账户余额。然后，大家一起记账，都写到一个账本（区块链）上，并且每个人都保留一份总账副本。

这个问题其实分两层，第一层是一个技术问题，并且已经有成熟的解决方案了，就是使用P2P技术（BT技术），大家都来同步分布式总账本，大家发送交易直接到节点，并且通过公私钥技术来验证节点；第二层是一个确认真实交易的问题，我们通过共识过程（consensus progress）来确认交易的有效性。目前有四种共识过程可以选择：工作量证明（POW）、权益证明（POS）、股份授权证明机制（DPOS）、验证池（POOL）。

第二是去掉特权参与者这个身份，如何去掉它又能保证资产的流通呢？这个问题也是一个核心问题。在公有链上，可以发行自己的虚拟货币，如bitcoin和litecoin。而在私有链的实现方式里，是将资产直接数字化，可以将对应的物理实体细分所有权发行。在图2中节点A直接发交易给节点D，所有节点一起确认并且验证交易的真实性，更新了公共总账以后，所有人再同步一下最新的总账。

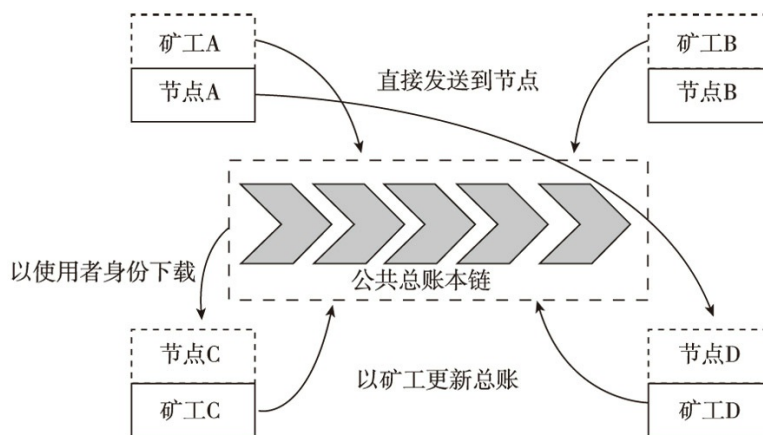


图2 区块链原理介绍2

资料来源：<https://www.zhihu.com/question/37290469/answer/79131321>

这里我们将维护者的身份下放至每一个参与者手中，并且通过加密算法来保证交易真实可信，不需要对账，只需要维护一条总账就可以。

1. 区块

Header: 链接到前面的块并且为区块链提供完整性

Body: 包含验证了块创建过程中的比特币交易的记录

2. 链

链目前分为三类：

（1）公有区块链（public BlockChains）

公有区块链是指世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是（目前）应用最广泛的区块链，各大bitcoins系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。

（2）联合（行业）区块链（consortium BlockChains）

联合（行业）区块链是指由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账。预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的API进行限定查询。

（3）私有区块链（private BlockChains）

私有区块链是指仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。截至2015年底，保守的巨头（传统金融）都是想实验尝试私有区块链，而公链的应用例如比特币已经工业化，私链的应用产品还在摸索当中。

如何建立一个严谨数据库呢？区块链的办法是将数据库的结构进行创新。顾名思义，区块链就是区块加链的方式组合在一起，以这种方式形成的数据库就是我们所谓的区块数据库。区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。

区块链是如何做到的呢？由于每一个区块的块头都包含了前一个区块的交易信息哈希值，这就使得从创始块（第一个区块）到当前区块连接在一起形成了一条长链。由于如果不知道前一区块的“交易缩影”值，就没办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。

“区块+链”的结构为我们提供了一个数据库的完整历史，从第一个区块开始，到最新产生的区块为止，区块链上存储了系统全部的历史数据；区块链为我们提供了数据库内每一笔数据的查找功能；区块链上的每一条交易数据，都可以通过区块链的结构追本溯源，一笔一笔进行验证；“区块+链+时间戳”是区块数据库的最大创新点，区块链数据库让全网的记录者在每一个区块中都盖上一个时间戳来记账，表示这个信息是这个时间写入的，形成了一个不可篡改、不可伪造的数据库。

（二）分散存储

分散存储是比特币的一个重要概念，它是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。区块链技术是应用程序基础，它超越了货币本身，这些技术能促进智能交易、分布式股权发布和资产转移。在未来，区块链技术可能会给我们货币交易、资产和数据进行带来变革。

1. 分布式存储系统

将数据分散存储在多台独立的设备上。传统的网络存储系统采用集中的存储服务器存放所有数据，存储服务器成为系统性能的瓶颈，也是可靠性和安全性的焦点，不能满足大规模存储应用的需要。分布式网络存储系统采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储信息，它不但提高了系统的可靠性、可用性和存取效率，还易于扩展。

2. 集群文件系统

是指运行在多台计算机之上，相互之间通过某种方式通信，从而将集群内所有存储空间资源整合、虚拟化并对外提供文件访问服务的文件系统。其与NTFS、EXT等本地文件系统的目的不同，前者是为了扩展性，后者运行在单机环境，纯粹管理块和文件之间的映射以及文件属性。集群文件系统有很多种。

（1）按照对存储空间的访问方式分类

可分为共享存储型集群文件系统和分布式集群文件系统。前者是多台计算机识别到同样的存储空间，并相互协调共同管理其上的文件，又被称为共享文件系统；后者则是每台计算机各自提供自己的存储空间，并各自协调管理所有计算机节点中的文件。Veritas的VxFS/VCS、昆腾的Stornext、中科蓝鲸的BWFS、EMC的MPFS都属于共享存储型集群文件系统。而HDFS、Gluster、Ceph、Swift等互联网常用的大规模集群文件系统无一例外都属于分布式集群文件系统。分布式集群文件系统可扩展性更强，目前已知最大可扩展至10K节点。

（2）按照元数据的管理方式分类

可分为对称式集群文件系统和非对称式集群文件系统。前者每个节点的角色均等，共同管理文件元数据，节点间通过高速网络进行信息同步和互斥锁等操作，典型代表是Veritas的VCS；而非对称式集群文件系统中，有专门的一个或者多个节点负责管理元数据，其他节点需要频繁与元数据节点通信以获取最新的元数据，比如目录列表文件属性等，典型代表是HDFS、GFS、BWFS、Stornext等。对于集群文件系统，其可以是分布式+对称式、分布式+非对称式、共享式+对称式、共享式+非对称式，两两任意组合。

（3）按照文件访问方式分类

集群文件系统可分为串行访问式和并行访问式，后者又被俗称为并行文件系统。串行访问是指客户端只能从集群中的某个节点来访问集群内的文件资源，而并行访问则是指客户端可以直接从集群中任意一个或者多个节点同时收发数据，做到并行数据存取，加快速度。HDFS、GFS、pNFS等集群文件系统，都支持并行访问，需要安装专用客户端，传统的NFS/CIFS客户端不支持并行访问。

（三）共识机制

1. 工作量证明（POW）

就是大家熟悉的挖矿，通过与或运算计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其他节点验证后一起存储；工作量证明机制（POW）不难理解，很多情况下我们都使用POW，只是不自知而已。在不考虑验证的情况下（无论是中心化还是非中心化的验证），我们可以认为任何具有概率性事件的累计都是工作量证明，如淘金。假设矿石含金量为 $p\%$ ，当你得到一定量黄金时，我们可以认为你一定挖掘了 $1/p$ 质量的矿石。而且得到黄金数量越多，这个证明越可靠。在一些其他场合我们也可以见到POW的踪影，比如电子游戏里的胜率、K/D比率，在大量的交战中一定的胜率能说明玩家的实力。同样有些游戏里的成就系统、装备体系也是POW，一般认为成就点数高的玩家在游戏里投入越多，越不容易诈骗，有时候交易点卡要求装备等级或者成就点数也是这个道理。因此，POW要求出示一定的证明表明工作量，证明可以是直接记录也可以是以概率表示，其中对于由小概率事件累计的工作，出示结果等同于证明了工作量（因为不太可能直接得到小概率结果）。在比特币和其他类比特币的系统中，POW系统是以合乎要求的HASH（哈希）作为工作结果。由于矿工要取得合法的计算结果需要一定量的计算，因此得到合法的计算结果就可以证明完成了一定量的计算。

优点：完全去中心化，节点自由进出。

缺点：目前比特币已经吸引全球大部分的算力，其他再用POW共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用。

2. 权益证明（POS）

POS是POW的一种升级共识机制，根据每个节点所占代币的比例和时间，等比例地降低挖矿难度，从而加快找随机数的速度。POS（Proof Of Stake）就是“股权证明”，即直接证明你持有的份额。除了混合性的PPC之外，真正的POS币是没有挖矿过程的，也就是在创世区块内就写明了股权证明，之后的股权证明只能转让，不能挖矿。在现实世界中股权证明很普遍，最简

单的就是股票。股票是用来记录股权的证明，同时代表着投票权和收益权。股票被创造出来以后，除了增发外，不能增加股权数量，要获得股票只能转让。在纯POS体系中，如NXT，没有挖矿过程，初始的股权分配已经固定，之后只是股权在交易者之中流转。股权从创世区块中流出，被交易者买卖而逐渐分散化。

优点：在一定程度上缩短了共识达成的时间。

缺点：还是需要挖矿，本质上没有解决商业应用的痛点。

3. 股份授权证明机制（DPOS）

DPOS是一种新的保障加密货币网络安全的算法。它在尝试解决比特币采用的传统工作量证明机制以及点点币和NXT所采用的股份证明机制的问题的同时，还能通过实施科技式的民主以抵消中心化所带来的负面效应。DPOS背后的基本原理是给持股人一把可以开启他们所持股份对应的表决权的钥匙，而不是给他们一把能挖矿的铲子。

DPOS的基本特点是持股人永远掌控大局，这样一来系统便是去中心化的。虽然投票的方式不够完美，但当涉及某事物（例如公司）的共同经营权时，这便是唯一可行的办法。幸运的是，如果你不喜欢公司的经营者，你可以抛售股份，而市场的反馈将促使持股人比一般群众更理性地进行投票。这样一来每一位持股人都能够选出某人，让他来代替持股人进行区块的签署（也可以称他为受托人）。任何能够获得超过1%选票的人都可以成为受托人，这些受托人便组成了“董事会”，并轮流签署区块。如果其中一位“董事”错过了签署该轮区块，客户端会自动将他的选票移走，因此错过签署区块的“董事们”将会被投出董事会，改由其他人加入。董事会成员会收到一些酬劳，以此作为他们进行竞选、担负风险、保证上线时间的工资。而他们也必须缴纳一小笔保证金，其金额相当于生产一个区块的收入100倍。要能够达成盈利，一位董事（受托人）必须保证99%以上的在线时间。

优点：最大化持股人的盈利；最小化维护网络安全的费用；最大化网络的效能；最小化运行网络的成本（带宽、CPU等）；大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：整个共识机制还是依赖于代币，很多商业应用不需要代币存在。

4. 验证池（Pool）

基于传统的分布式一致性技术，加上数据验证机制，是目前行业链大范围在使用的共识机制。

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Paxos、Raft）基础上，实现

秒级共识验证。

缺点：去中心化程度不如比特币；更适合多方参与的多中心商业模式。

二、区块链的核心特点

（一）开放

比特币的本质是一个互相验证的公开记账系统。这个系统所做的事情，就是记录所有账户发生的所有交易。每个账号的每笔数额变化都会记录在全网总账本（区块链）中。而且每个人手上都有一份完整的账本，每个人都可以独立统计出比特币有史以来每个账号的所有账目，也能算出任意账号当前余额是多少。比特币客户端在使用时会进行大量的数据同步，它同步的就是全网总账本，这些数据保障了整个体系的去中心化和每个客户端的一切知情权。正是因为所有数据公开透明，而整个比特币软件也是开源的，任何人都可以去查看它的源代码，人们才会信任这套去中心化的系统，而不担心里面是否隐藏着什么阴谋。

开放交易的一个主要目的是将所有金融资产分散化，通过密码学加密所有的人都可以发布货币和各种金融资产。任何人都可以在开放的交易中创建数字标记，这些标记代表实际的价值。这个最具创新特性是一旦某人发布了这个数字标记后，他就不能在全球账单中改变他们的货币或者股份。比特币交易中开放性的好处是无国界、跨境。跨国汇款会经过层层外汇管制机构，而且交易记录会被多方记录在案，但如果用比特币交易则直接输入数字地址，点一下鼠标，等待P2P网络确认交易后，大量资金就过去了，不经过任何管控机构，也不会留下任何跨境交易记录。

开放交易也有一些缺点，它们的表现和比特币不一样，这意味着被比特币社区所接受将更缓慢，而基于比特币系统的东西更容易被社区接受。

（二）分布式

区块链技术也被称为分布式账本技术。分布式账本从实质上说就是一个可以在多个站点、不同地理位置或者多个机构组成的网络里进行分享的资产数据库。在一个网络里的参与者可以获得一个唯一、真实账本的副本。账本里的任何改动都会所有的副本中被反映出来，反应时间会在几分钟甚至是几秒内。在这个账本里存储的资产可以是金融、法律定义上的，实体的或是电子的资产。在这个账本里存储的资产的安全性和准确性是通过公私钥以及签名的使用去控制账本的访问权，从而实现密码学基础上的维护。根据网络中达成共识的规则，账本中的记录

可以由一个、一些或者是所有参与者共同进行更新。

区块链就是这种分布式账本的底层技术，它最初是为在2008年实现的点对点数字现金系统比特币而设计的。区块链算法让比特币的交易可以在“区块”里集中起来，并通过密码学签名添加到现有区块组成的“链”里面。比特币账本是用分布式及“无须许可”的方式构建的，任何人都可以通过解决生成新区块所需的密码学难题从而添加一个包含交易的区块。这个系统的鼓励机制是在解决难题并生成每个区块后得到25个比特币的奖励。任何人只要有网络和电脑的算力，都有机会解决这些密码学难题并将交易添加到账本里，这些人被称为“比特币矿工”。挖矿的比喻是很恰当的，因为比特币的挖掘是要消耗大量的电脑运算能力，因此会带来很高的能源消耗。据估计，比特币网络运行所需的能源超过1GW（十亿瓦特），可以与爱尔兰的电力消耗相提并论了。

分布式账本技术有潜力帮助政府征税、发放福利、发行护照、登记土地所有权、保证货物供应链的运行，并从整体上确保政府记录和服务的正确性。在英国国民健康保险制度（NHS）里，这项技术通过改善和验证服务的送达以及根据精确的规则去安全地分享记录，有潜力改善医疗保健系统。对这些服务的消费者来说，这项技术根据不同的情况，有潜力让消费者们去控制个人记录的访问权并知悉其他机构对其记录的访问情况。

现行的数据管理方案，特别是个人数据的管理，通常是在单一的机构内架设的大型传统IT系统。由此还会引入一系列的网络与通信系统，才能实现与外界的交流，这也增加了额外的成本和复杂性。高度中心化的系统的单点失败的概率很高。这也会带来被黑客攻击的风险，而数据经常会出现没有及时同步的、过期的或者不准确的问题。

与此相反，分布式账本天生就是很难被攻击的，因为它没有用单一的数据库去存储记录，而是保留了同一个数据库的多个副本，因此黑客攻击必须同时针对所有的副本才能生效。这个技术也具备阻止未经授权修改或恶意篡改的能力，因为网络中的参与者会立刻发现账本中的某个部分被篡改了。另外，这种技术用于维护信息安全及更新信息意味着参与者可以共享数据，并确保账本的所有副本在任何时候都是与其他副本一致的。

不过，这不代表分布式账本对黑客攻击是免疫的，从原则上说，任何人只要能够找到“合法”地修改一个副本的方法，则有可能修改账本的所有副本。因此，保证分布式账本的安全性是一项重要的任务，就如确保现代社会运行所依赖的数字技术基础设施的安全性一样。

商业界很早就看到了这项技术的潜力。分布式账本提供了一种确保商品及知识产权的所有权和起源的新方法。例如，Everledger提供了一种确保钻石身份的分布式账本，并记录从采掘、切割、销售和承保的相关信息。在这个有相当多的纸质文件被伪造的市场里，这种技术让钻石的归类更加高效，并有潜力降低诈骗的风险，以及防止“血腥钻石”（即在战乱或冲突地区开采并用于资助战争活动的钻石贸易）进入市场。

总的来说，分布式账本技术提供了一个框架，让政府可以用于减少欺诈、腐败、错误和涉及大量纸质文件业务的耗费。它有潜力重新定义政府与公民在数据分享、透明度和信任意义上的关系。对私营部门来说，类似的潜力也是存在的。

（三）总账本

可以把区块链想象成一个比特币的公共账本，这个账本：（1）里面记录着自比特币诞生以来的所有比特币转账交易（即总账）；（2）存放在互联网的各个比特币节点上，每个节点都有一份完整的备份；（3）是分区块存储的，每一块包含一部分交易记录，每一个区块都会记录着前一区块所有交易信息的哈希值，形成一个链状结构，因而称为区块链；（4）当你要发起一笔比特币交易的时候，只需把交易信息广播到P2P网络中，矿工把你的交易信息记录成一个新的区块连到区块链上，交易就完成了。

1. 公共账本的特征

（1）去中心化。整个账单网络不需要中心管理系统或机构，个体与个体之间能够有效实现信息共享，有效提高数据存储和运行速度。现在交易模式是交易个体将信息传输到中央服务器，再由中央服务器经过数据分析，返回到交易个体。而区块链则可以实现网络个体两两互动，交易信息就在他们之间直接传递，不再上传到中央服务器，大大降低了交易的运行时间，提高了效率。

（2）每次交易产生的账本都记录在区块链的节点上，每个账本都有完整的备份。

（3）每个账本都记录着本次交易及以前所有交易的所有信息，通过这种方式，从账本最初状态开始，每一张账单记录是公开可验证并有时序，当前每个人持有的资产数等信息都是可以被推算出来的。

（4）区块链实现了两种记录：交易以及区块。交易的是被存储在区块链上的实际数据，而区块则是记录确认某些交易是在何时，以及以何种顺序成为区块链的一部分。交易是由参与者在正常过程中使用系统所创建的，而区块则由“矿工”负责创建。

（5）当你要发起一笔交易时，需把交易信息广播到区块链网络中，“矿工”把交易信息收录并验证合法后，交易就完成了。

（6）对于试图修改或者重写交易记录的人而言，这个成本是非常高的。在数据和用户量低的时候相对容易通过，但如果数据和用户量非常大，想要通过修改就将非常困难，别人不认可，你的修改就没有意义。

2. 关于公共账本的三个问题

第一个问题：如何保证用户有足够的余额？例如你只有10个币，而你居然发起了一笔转20个币的交易怎么办？这个问题很好解决，因为区块链上记录了所有比特币交易记录，只需要回溯所有的和你账户相关的历史交易就能知道你这个账户上到底有多少余额，余额不对的账户矿工是会拒绝记录你的交易的。由此可能又会产生一个疑问，那么最初的比特币是从哪里来的呢？最初的比特币是由系统奖励给记录区块的矿工的。每一个区块在生成的时候就会在生成这个区块的矿工的账户上生成一定数量的新比特币作为奖励。

第二个问题：如何保证你的账户不被冒名顶替？这个问题也很好解决，用数字签名技术就可以了。每个比特币账户都有公钥和私钥，你发起交易的时候用私钥对交易信息签名，矿工收到信息后用公钥检查一下签名就可以。

第三个问题：那么多矿工，如何决定该由哪个矿工生成下一个区块？解决方案是这样的：中本聪设计了一个数学问题，这个数学问题会耗费大量的计算机cpu时间才能得出答案，同时每一次得出的答案都会作为下一次计算的初始条件。全世界的矿工一起来计算这个问题，谁先得出答案，谁就可以用这个答案生成一个新的区块，再广播到网络中。收到这个新块数据的矿工会立即停止当前的计算，用新块里的数据重新进行下一次计算。这就是所谓的“挖矿”。矿工产生的区块一旦被网络接受，他就能获得一笔比特币作为酬劳。这时要考虑一种情况：如果同时有两个矿工各自得到一个正确答案，并各自生成了一个区块广播出去会发生什么呢？这时在区块链上同一个位置就有了两个区块，所谓的“分叉”就出现了。分叉是绝对不允许的，所以当矿工发现区块链分叉之后，会选择最长的一条继续计算，短的那条区块链会被丢弃。

仔细思考下这个体系，你会发现它几乎无懈可击。首先你不能凭空造出比特币，只能挖矿获得；其次你无法伪造交易，无法控制不属于你的账户；最后交易一旦被确认，几乎无法取消。

总体来看，区块链数据库系统是一个公共总账本，全球一本账，所有的数据记录在这一本账上。比如，我们可能在不同的银行开了不同的账户，不同的银行账户被不同的银行所记账，但是没有一个系统可以提供一本总账给你。你在不同银行的所有账户到底有多少钱、欠了多少钱、每个月要付多少利息，需要你自己来计算。在区块链这个数据库，全球一本总账，这个账是公开透明的。维护、存储这个账本数据库，使用的是共识算法，这个数据库里面所有的账不是由你本人来记账，而是由第三方记账的。你本身无法篡改它，因为你的篡改不会被别人认可，除非你串通网上的所有人都帮助你记假账，这需要你控制这个网络超过51%的节点或者计算能力，你才可能在网上做假账，但这几乎是不可能完成的事情。如果要完成的话，成本也非常高，高到你做假账根本不划算。共识算法确保了这个数据库不可篡改，不能作伪，并且可追溯。即使50%的东西坏了，这个数据库还能继续有效地运行。同时，这个数据库的安全保障是

非对称的加密算法，到目前为止，没有一个黑客有能力成功攻破过任何一个比特币账户，因为无法破解它。因此，从数据库的层面，区块链和现有金融体系及金融机构的数据库相比，具有很大的潜力和价值。

经过无数次的记账，区块链就成为一个可信赖、超容量的公共账本。

三、区块链的核心原理

（一）点对点传输

点对点技术（peer-to-peer，简称P2P）又称对等互联网络技术，是一种网络新技术，依赖网络中参与者的计算能力和带宽，而不是依赖放在较少的几台服务器。P2P网络通常用于通过Ad Hoc连接来连接节点，这类网络可以用于多种用途，各种文件共享软件已经得到了广泛的使用。P2P技术也被使用在类似VoIP等实时媒体业务的数据通信中。

纯P2P网络没有客户端或服务器的概念，只有平等的同级节点，同时对网络上的其他节点充当客户端和服务器。这种网络设计模型不同于客户端——服务器模型，在客户端——服务器模型中通信通常来往于一个中央服务器。有些网络（如Napster、OpenNAP或IRC @find）的一些功能（比如搜索）使用客户端——服务器结构，另一些则使用P2P结构来实现另外一些功能。类似Gnutella或Freenet的网络则使用纯P2P结构来实现全部的任务。

1. 点对点传输的优势

P2P网络的一个重要的目标就是让所有的客户端都能提供资源，包括带宽、存储空间和计算能力。因此，当有节点加入且对系统请求增多时，整个系统的容量也增大。这是只有一组固定服务器的客户端——服务器结构不能实现的，因为在上述这种结构中，客户端的增加意味着所有用户更慢的数据传输。

P2P网络的分布特性通过多节点上复制数据，也增加了防故障的强度，并且在纯P2P网络中，节点不需要依靠一个中心索引服务器来发现数据。在后一种情况下，系统也不会出现单点崩溃。

当用P2P来描述Napster网络时，对等协议被认为是重要的，但是实际中，Napster网络取得的成就是通过对等节点（就像网络的末枝）联合一个中心索引来实现。这可以使它能快速并且高效地定位可用的内容。对等协议只是用一种通用的方法来实现这一点。

有些网络和通信渠道，像Napster、OpenNAP和IRC@find，一方面使用了主从式架构结构来

处理一些任务（如搜索功能），另一方面又同时使用P2P结构来处理其他任务。而有些网络，如Gnutella和Freenet，只使用P2P结构来处理所有的任务，有时被认为是真正的P2P网络。尽管Gnutella也使用了目录服务器来方便节点得到其他节点的网络地址。

2. 点对点传输应用

宾夕法尼亚州立大学的开发者联合麻省理工学院、西蒙弗雷泽大学的研究人员，还有第二代互联网P2P工作组，正在开发一个P2P网络的学术性应用。这个项目被称为LionShare，是基于第二代网络技术，更详细地说是Gnutella模型。这个网络的主要目的是让众多不同学术机构的用户能够共享学术材料。LionShare网络混合了Gnutella分散的P2P网络和传统的C/S网络。这个程序的用户能够上传文件到一个服务器上，不管用户是否在线，都能够持续地共享。这个网络也允许在比正常情况下小得多地共享社区中使用。与当前正在使用的其他P2P网络的主要不同是，LionShare网络不允许匿名用户。这样做的目的是防止版权材料在网络上共享，这同时也避免了法律纠纷。另一个区别是对不同用户有选择性地共享个别的文件。用户能个别选择哪些用户可以接收这一个文件或者这一组文件。学术社区需要这种技术，因为有越来越多的多媒体文件应用在课堂上。越来越多的教授使用多媒体文件，如音频文件、视频文件和幻灯片。把这些文件传给学生是件困难的任务，而如果用LionShare这类网络则容易得多。

（二）分布式公共网络

分布式计算技术处于多种方案并存的现象，RMI（远程方法调用）是平台独立的，但它不是编程语言独立的技术，客户机和服务器代码必须用Java来编写；对于DCOM，它语言虽然是独立的，但平台不是独立的，虽然程序可以使用许多不同的编程语言，但是它只能运行在Microsoft家族的操作系统上。CORBA同时能够做到编程语言和运行平台的独立性，但是基于CORBA的系统必须通过ORB进行通信。于是就出现了SOAP这样一种不捆绑任何一种硬件平台、操作系统、编程语言或网络硬件的分布式计算方案。

分布式网络拓扑结构一般呈网格状，和集中式网络结构不同，节点间不再是点对点的通信方式。通信方式的这种改变使得客户机/服务器的网络模型和网络的计算信息处理模型更易于分布式地实现。在分布式网络结构中，数据处理中心的概念已经淡化了，因为每一个网络站点既是网络服务对象又是网络服务提供者。

1. 分布式网络结构和集中式网络结构相比的优点

（1）电缆长度短，连线容易。因为任何一个想入网的计算设备只需就近连入网络，而不必直接连到中央节点。

（2）可靠性高。网状拓扑结构保证了冗余度，因为在任何两个节点之间至少有两条链路，

所以当一个站点失效或者一条链路中断时，网络其他站点的通信不受影响。

(3) 易于扩充。增加新的站点 (site) 可以在网络的任何点将其接入。

2. 分布式网络结构的缺点

(1) 建网复杂，网络难于管理。

(2) 故障诊断困难。分布式结构的网络不是集中控制，故障检测只能逐个检查各个站点。

(3) 需要更多的网络技术人员和管理人员。因为各个站点彼此分散，而且每个站点的维护、管理工作都不简单；需要配备网络专业技术人员定期进行维护，有必要的话还需专职人员进行日常维护和管理。

(三) 加密货币发行

1. 虚拟货币分为非加密货币和加密货币

(1) 非加密货币是由公司或者私人自我固定发行，可无限发行，不需要通过计算机的显卡运算程序解答方程式获得。知名的虚拟货币如百度公司的百度币、腾讯公司的Q点、盛大公司的点券、新浪推出的微币（用于微游戏和新浪读书）等，因为其依据市场需求可无限发行，所以不具备收藏及升值价值。

(2) 加密货币不依靠法定货币机构发行，不受央行管控。它依据全世界的计算机运算一组方程式开源代码，通过计算机显卡、CPU大量的运算处理产生，并使用密码学的设计来确保货币流通的各个环节安全性。基于密码学的设计可以使加密货币只能被真实的拥有者转移或支付。

(3) 加密货币与其他非加密虚拟货币最大的不同是其总数量有限，具有极强的数量稀缺性。因为这一组方程式开源代码总量是有限的，必须通过计算机显卡的运算才可以获得。

(4) 正因为加密货币总量有限，具有稀缺性，所以开采越多，升值越高，就好像地球上埋在地里的黄金，数量有限，永不贬值。我们计算机运算方程式代码的这一个运算过程就好比在金矿挖矿。

(5) 加密货币长什么样子：通过挖矿开采出来后，加密货币就是一串代码，跟人民币左下角的那一串序列号一样，谁拥有这一串序列号，谁就拥有这一加密货币的使用权。

2. 加密数字货币的核心是其能成为各国货币之间的媒介

它最终起到的是“国际物联网、贸易之间的结算、结汇”作用。虚拟货币之所以引起全球众多领域的关注，是因为它正在制造一个全球的快流通，并且流通领域越大、范围越广、其使用价值越高。因此虚拟货币的发行必须是在全球化领域发行。并且，从公司平台上能看到流通领域和市场份额，发行商亦正在通过努力拓宽其流通领域的市场空间或平台向此目标迈进。

3. 加密数字货币流通必须经得起各国法律的推敲和考证

比如虚拟货币发行不能成为恐怖主义、非法组织机构洗钱、逃税漏税的工具，虚拟货币发行从长远趋势看必须能被轻松纳入各国金融体系和税收管理，虚拟货币才有足够的市场空间和升值空间。这就要求虚拟货币发行管理必须实名化登记，类似比特币之类的匿名发行方式将成为其去中心化发展的一大障碍。

4. 加密数字货币的发行是一种突破

加密数字货币的发行有利于增加社会融资渠道、降低国际融资门槛、拓宽社会融资市场，其直销繁衍的众筹方式是从社会底层收入抓起的一种经济方式。其最大的助益是缩小贫富悬殊，提倡人人参与，为社会各界提供一个共荣的平台。因此虚拟货币发行模式必须受众面够广。比特币价格高企，已经不适合一般人去投资，而易物币的发行模式受众面更广，对推动底层经济较为助益。

5. 投资者、大众消费者、使用者必须有货币战争的意识，有全球性视野

因为各国都寄希望于自己国家的虚拟货币能充当未来支付媒介系统，毕竟这是一场全球化领域的经济战。虽然从表象看虚拟货币目前是介于企业之间的战争。但从实质看，虚拟货币已经成为国家与国家之间主导的一场暗战。

（四）去中心化

去中心化可能会在某些领域具备巨大竞争优势。去中心化不代表没有中心，只是将中心从“人”这种不可控的因素中移至可控并且中立的因素中，这样之前的竞争优势就不会存在。因此从某种意义上来说，去中心化是一个“降权”的操作，同时对于个人而言可控性更好。经过这样的操作后整个网络形态会成为一个“细胞组织”，它们互相很难受到影响，因而更加稳定，但同时面临了新鲜空气进入困难的问题。去中心化是一个社会学操作，但是更优秀的处理思路可能会来自生物学或者其他学科。去中心化对中层用户更有价值，中层用户可以通过迅速成长，拥有自己的话语权。去中心化的益处在于，能够展现出更多有价值的小中心，有人的地方就必然有中心，只是聚合半径大小的问题。

1. 去中心化的优点

（1）可适应性——就像人的脑袋一样，即使部分区域失去效果（像失忆和失语），但不影响脑袋的整体运行，部分不影响整体。

（2）可进化性——像DNA、电脑系统一样可以不断升级。

（3）无限性——这是一套并行运行系统，所以会有冗余部分，它的自我延伸性和自动繁衍性是永无止境的。

（4）弥补性——无规则组合会产生无数的可能性，同时又不强调个体的重要性，就算个体有缺陷和不足也不会导致整体的不足。

2. 去中心化的缺点

（1）并非最优——存在冗余又没有中央控制，有时效率是低下的，资源分配是混乱的。如蚂蚁搬家时的混乱，但它最终又会走向有序。

（2）不可控制——没有绝对领导和权威，所带来的后果就像放出去的羊，被狼吃掉的可能性很大。也像癌细胞，你永远杀不死它，它会自动调整。

（3）不可预测——像微博上的一件小事件，通过这种网状传播，它的效应被无限扩大化，成了流行或热点事件。

（4）不可知——分布式的去中心化是一种横向因果关系，A影响其他，其他影响A，一切像网一样散开传播和产生影响。

（5）重启效应差——点火系统很好，但机械的预热时间很长，并且要有足够的影响力和传播率。每个个体必须找回到自己的所在位置，各就各位才行。

参考文献

- [1] 拜占庭将军问题 [G/OL]. 维基百科.<https://zh.wikipedia.org/wiki/>.
- [2] 微软亚洲研究院. 莱斯利兰伯特荣获2013年图灵奖[EB/OL]. <http://msra.cn/zh-cn/news/features/leslie-lamport-turing-20140327.aspx>.
- [3] 兰伯特等. 拜占庭将军问题[EB/OL]. <http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf>.
- [4] 中本聪. 比特币：点到点的电子现金系统[EB/OL]. <https://bitcoin.org/bitcoin.pdf>.
- [5] Blockchain. 比特币区块链中最近开采出的区块[EB/OL]. <https://blockchain.info/>.
- [6] <https://bitcointalk.org/>
- [7] <http://coinmarketcap.com/>
- [8] 千家驹, 郭彦岗. 央行数字货币猜想[EB/OL]. <http://quant.dataguru.cn/article-9074-1.html>.
- [9] 肖风. 区块链来了, 数字货币逼近, 美国英国德国早已行动, 中国跟进[EB/OL]. http://www.thepaper.cn/newsDetail_forward_1453413.
- [10] 董俊峰. 美国的Fintech与中国的互联网金融有何不同[EB/OL]. <http://finance.eastmoney.com/news/1373,20160314603873932.html>.
- [11] 华尔街见闻. 全球Fintech公司商业模式梳理: 用这四条策略你就能赢[EB/OL]. <http://money.163.com/16/0304/17/BHB52S6L00253B0H.html>.数据来源CB Insights data.
- [12] 区块链1.0: 货币[EB/OL]. <http://www.8btc.com/blockchain-and-currency>.
- [13] 区块链2.0: 智能合约[EB/OL]. <http://www.8btc.com/blockchain-smart-contract>.
- [14] 巴比特.R3CEV[EB/OL]. <http://www.8btc.com/r3cev>.
- [15] 有史以来规模最大的区块链试验, R3说这只是个开始[EB/OL]. <http://www.8btc.com/r3-blockchain-trial>.

- [16] printemps.巴比特[EB/OL]. <http://www.8btc.com/r3-add-12>.
- [17] printemps.巴比特[EB/OL]. ING高管：我行全面探索区块链，如无效果则放弃
<http://www.8btc.com/ing-blockchain>.
- [18] 超级账本（HYperledger）技术委员会成员首度曝光[EB/OL].
<http://www.8btc.com/hyperledger-tsc>.
- [19] 巴比特[EB/OL]. <http://www.8btc.com/wall-street-blockchain-2>.
- [20] 国际汇款三大便利新路径银行汇款哪家最省钱. 理财周刊[EB/OL].
<http://baike.so.com/doc/5409553-5647579.html>, western union.
- [21] 银行结算系统 [G/OL] . 百度百科.
<http://baike.baidu.com/subview/61075/13876198.htm>
- [22] 瑞波币追随比特币来中国淘金[EB/OL]. <http://finance.qq.com/zt2014/focus/ripple.html>.
- [23] 瑞波币 [G/OL] . 360百科. <http://baike.so.com/doc/9504067-9847602.html>.
- [24] 证券结算 [G/OL] . 百度百科. <http://baike.baidu.com/link?url=TfntnBRcnWnRHUZjUR16yFM5lrkhmgBqM5yMZfXIBpmeBXy6Z5fwj9UER5IHmY68>.
- [25] 证券清算 [G/OL] . 百度百科. http://baike.baidu.com/link?url=cpx7dli6HXrj3h-zb27NVHX3ifHoKnCpnLObt7Ov3rZNJn7Ma_K5JqifEk9dR2FKGSlzkcZ3z91PNph9kIc9Dq.
- [26] 丁化美，费兰静. 国际证券交易结算方式比较[EB/OL].
<http://finance.jrj.com.cn/2011/04/2510339813149-1.shtml>.
- [27] 巴比特. 区块链在资本市场应用的深入探讨[EB/OL]. <http://www.8btc.com/blockchain-in-capital-markets>.
- [28] 区块链咨询. 德勤为央行做的区块链报告都说了些啥[EB/OL].
<http://www.8btc.com/535352>.
- [29] Adrian Lee, KiHoon Hong. 区块链技术变革股票市场交易的挑战和局限[EB/OL].
<http://chainb.com/?P=Cont&id=288>.
- [30] Anna Irrera.区块链帮助实现股票T+0交易后面临的5个难题[EB/OL].
<http://chainb.com/?P=Cont&id=324>.

[31] 2014年国内数字货币行业发展报告[EB/OL]. http://iof.hexun.com/2015-02-28/173620489_8.html.<http://chainb.com/?P=Cont&id=235>.

[32] 股权众筹模式风生水起[EB/OL]. <http://mt.sohu.com/20150731/n417921784.shtml>.

[33] 郭勤贵. 中国式股权众筹二十大问题[EB/OL]. <http://iof.hexun.com/2015-09-02/178807796.html>.

[34] Entrepreneur.加密股权：未来众筹领域新风向标[EB/OL].
<http://www.weiyangx.com/43318.html>.

[35] 区块链上的P2P票据交易所呼之欲出[EB/OL].
<http://www.tui18.com/a/201601/28109754.shtml>.

[36] 2015年票据市场分析及2016年票据市场展望[EB/OL].
<http://news.163.com/16/0115/16/BDCQKHRT000146BE.html>.

[37] 去官僚化的信贷革新者：第一家比特币P2P借贷平台BTCJam[EB/OL].
<http://36kr.com/p/218242.html>.

[38] 农行39亿后，区块链上的P2P票据交易所呼之欲出[EB/OL].
<http://www.sinotf.com/GB/News/1001/2016-02-12/0NMDAwMDE5NzY0NA.html>.

[39] 审计的基本定义[G/OL]. 百度百科. <http://baike.baidu.com/link?url=vYE13vIZZViZbA9e3A-sO12ZvbWv1kAVJIISBTOnbulRegOzBjYCBY5xlqAe0xjb8mCIg203swyZsLyDD86j78BsEQncVh1Q>

[40] 社会审计的定义[G/OL]. 百度百科. http://baike.baidu.com/link?url=liDTX4NqPk0bLFeUl5KvWNBPTyDWEwF6fXrWRRshZf2RPFaWDo0bp7cxISbsF4_n

[41] 安然、安达信事件冲击波的思考[EB/OL]. <http://lxp.cai.swufe.edu.cn/245.htm>.

[42] “区块链”技术深刻影响金融业[EB/OL]. <http://it.sohu.com/20160111/n434175506.shtml>.

[43] 熊纯倩. 德勤试验区区块链技术，提升客户审计服务[EB/OL].
<http://www.8btc.com/deloitte-blockchainhttp://finance.huanqiu.com/zl/2015-10/7789840.html>.

[44] 熊纯倩. 德勤试验区区块链技术，提升客户审计服务[EB/OL].
<http://toutiao.com/a4723987774/>

[45] Alex Fowler.比特币公司Blockstream与普华永道达成战略合作关系[EB/OL].

<http://www.8btc.com/pwc-and-blockstream>.

[46] 去中心化[G/OL]. 微百科. <http://www.baike.com/wiki/>.

[47] Florian Glatz. 什么是智能合约? 智能合约解析[EB/OL]. <http://www.wanbizu.com/baike/201412144027.html>.

[48] Richard Brown. 一个简单的智能合约模型[EB/OL]. <http://www.8btc.com/model-smart-contracts>.

[49] Michael Halloran. 银行业之后, 区块链又要颠覆物联网[EB/OL]. <http://www.8btc.com/blockchain-and-the-internet-of-things>.

[50] Kyle Rootstock. 与以太坊的战斗究竟谁能胜出[EB/OL]. <http://www.8btc.com/rootstock-contests-ethereum-for-smart-contracts-domain>.

[51] 巴比特[EB/OL]. <http://www.8btc.com/lightning-network>.

[52] Peterhon. 闪电网络与以太坊结合建立支付渠道的构想及其前景[EB/OL]. <http://www.8btc.com/ethereum-lightning-network>.

[53] John Ratcliff. 闪电网络非常伟大, 但它也面临各种类型的问题[EB/OL]. <http://www.8btc.com/lightning-network-so-great>.

[54] 199IT. 分布式账本技术: 超越区块链[EB/OL]. <http://mini.eastday.com/a/160313145632859.html?btype=index&subtype=keji&idx=0&ishot=0>.

[55] 什么是中心化和去中心化[G/OL]. 知乎. <http://www.zhihu.com/question/19744551>.

[56] 区块链的原理是什么[G/OL]. 知乎. <http://www.zhihu.com/question/31112808>.

[57] 区块链[G/OL]. 百度百科. http://baike.baidu.com/link?url=NbsbjLMO_KBpiY1vIFCAewEtIsCvjiu_UrQbeBwb27CqOrZqGxo2nzdrpBHYuXKoE52fv2AJr-mj6V9sU0TrJK.

[58] 区块链是什么, 如何简单易懂地介绍区块链[G/OL]. 知乎. <https://www.zhihu.com/question/37290469/answer/79131321>.

[59] Vitalik Buterin. 漫谈公共区块链和私有区块链[EB/OL]. <http://news.hexun.com/2016-01-07/181654921.html>.

[60] cywosp. 分布式存储及应用[EB/OL]. <http://blog.csdn.net/cywosp/article/details/7453529>.

[61] 区块链目前用到哪些共识机制？它们各自的优缺点和适用范围是什么[G/OL]. 知乎.
<http://www.zhihu.com/question/30921471/answer/79209219>

[62] 点对点传输[G/OL]. 百度百科. http://baike.baidu.com/link?url=YPNc-zBJ2buwyr1P-mW5LqIuhqgbc4oUs3J-lEpKUZjpO-ZEapPl5gfPBgoTSCfSOPasg7AxbXhOqDHtD_JRV_.

[63] 分布式公共网络[G/OL]. MBA智库百科. <http://wiki.mbalib.com/wiki/>.

[64] 什么是加密货币[EB/OL]. <http://blog.3g.cnfol.com/tytdcyl/article/1446618905-109158811.html>.



图书在版编目（CIP）数据

区块链：重塑经济与世界 / 徐明星等著.—北京：中信出版社，2016.6

ISBN 978-7-5086-6211-4

I. ①区... II. ①徐... III. ①电子商务—支付方式—研究 IV. ①F713.36

中国版本图书馆CIP数据核字（2016）第102180号

区块链：重塑经济与世界

著 者：徐明星 刘勇 段新星 郭大治

策划推广：中信出版社（China CITIC Press）

出版发行：中信出版集团股份有限公司

（北京市朝阳区惠新东街甲4号富盛大厦2座 邮编 100029）

（CITIC Publishing Group）

中信出版社官网：<http://www.citicpub.com/>

官方微博：<http://weibo.com/citicpub>

更多好书，尽在中信书院

中信书院：App下载地址<https://book.yunpub.cn/>（中信官方数字阅读平台）

微信号：中信书院